金融行业

7 月报
2021 年

# 安全月报

安全观点 | 行业研究 | 漏洞聚焦 | 安全态势

绿盟科技金融事业部出品

## 安全观点

零信任架构助力实现智慧安全3.0可信访问

## 行业研究

《网络安全审查办法（修订草案征求意见稿）》解读

打个样 | 如何更好地践行《网络产品安全漏洞管理规定》?

攻防论道之保障篇 | 克难制胜，攻防对抗之五步保障要领

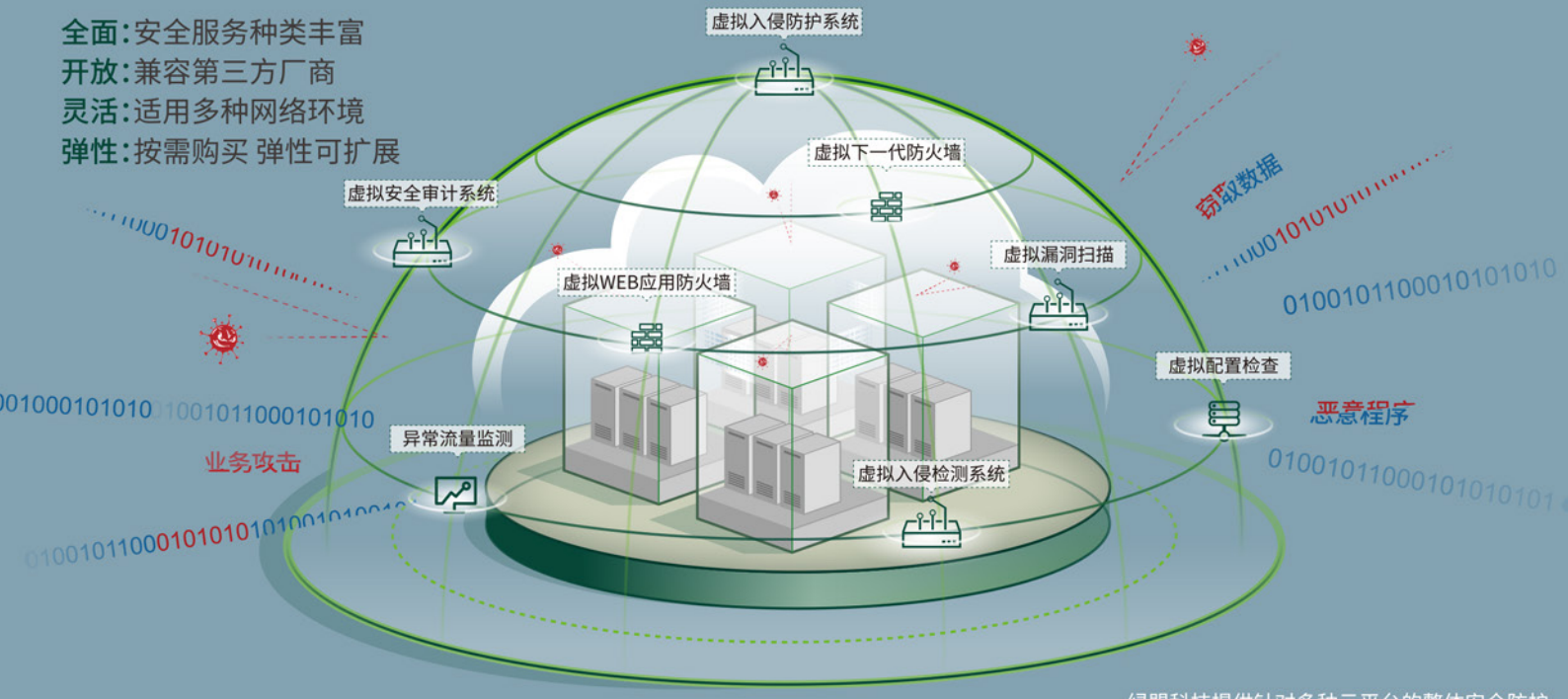
Android 银行木马 Toddler 针对欧洲银行用户开展攻击活动

美国橡树岭银行披露数据泄露事件

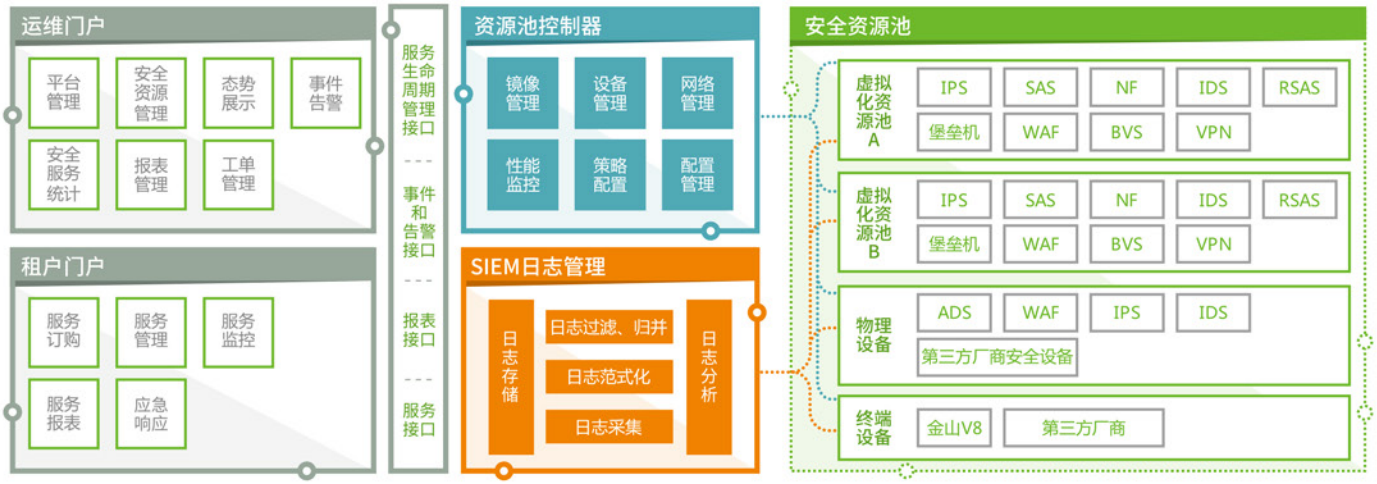
NSFOCUS

# 绿盟科技
# 云计算安全解决方案

全面:安全服务种类丰富
开放:兼容第三方厂商
灵活:适用多种网络环境
弹性:按需购买 弹性可扩展




绿盟科技提供针对多种云平台的整体安全防护





**THE EXPERT**
**BEHIND GIANTS**
**巨人背后的专家**

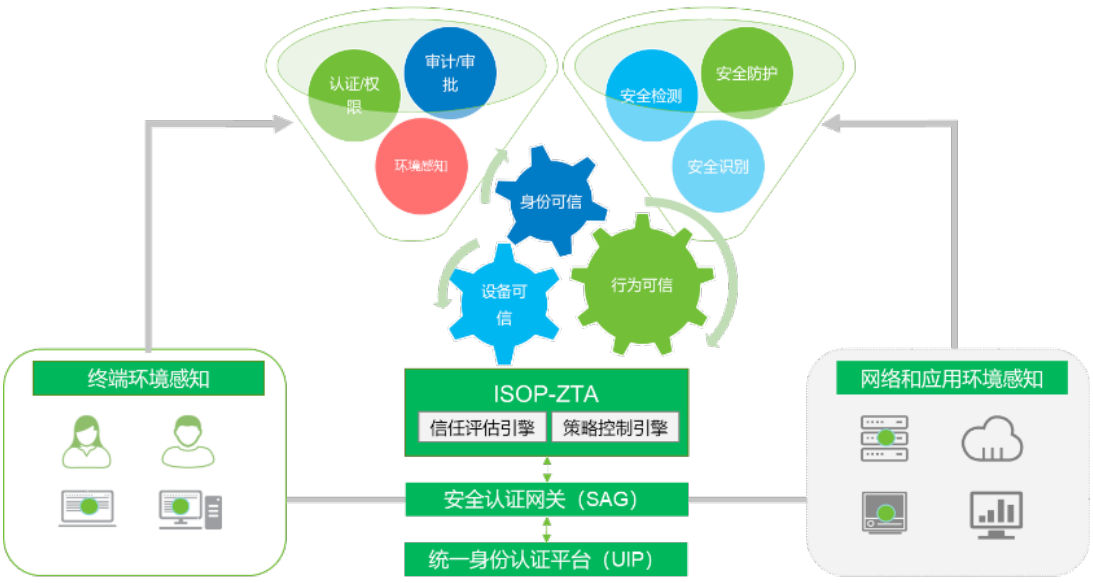
多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

# 本|期|看|点

## P04 零信任架构助力实现智慧安全 3.0 可信访问




## P08 《网络安全审查办法（修订草案征求意见稿）》解读

# 安全月报

2021年第7期

绿盟科技金融事业部

# 目录 CONTENTS



安全月报在线阅读

绿盟科技官方微信

NSFOCUS

# 安全观点

# 零信任架构助力实现智慧安全 3.0 可信访问
## 构建可信任网络环境

田旭达

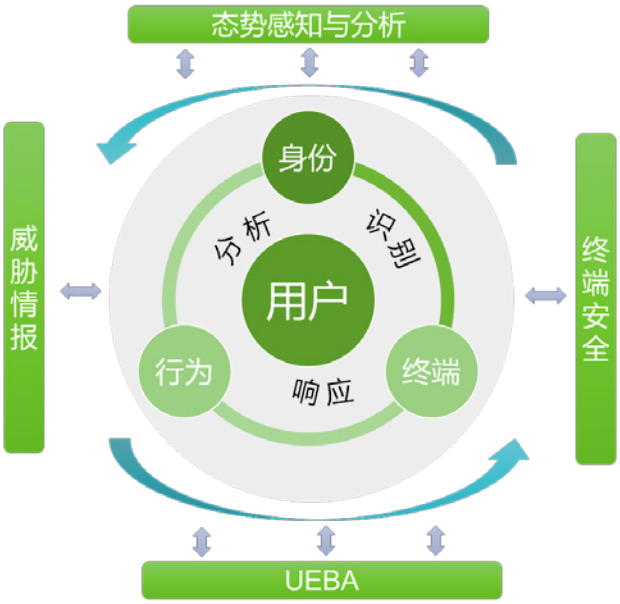
5G、云计算、人工智能、物联网、工业互联网等新基建的快速融合发展不断模糊网络的安全边界。随着网络安全形势的不断演进，针对信息系统的网络安全威胁环境也发生了重大变化，勒索软件，0-Day漏洞，高级持续性威胁已成为当前的主流攻击形式。网络安全攻击已逐步形成组织严密、技术精湛的团队化作战，攻击者的不对称性优势，也一直是安全团队面临的最大问题。在当前这种攻防失衡的局势中，传统的基于边界安全防护，单次静态安全策略配置的安全措施已经无法满足业务发展的安全需求，网络安全产业面临着新一轮技术更新换代所带来的挑战和发展机遇。

绿盟科技基于当前形势，以及对网络安全面临的新挑战的观察和对未来发展的深度思考，提出了构建“全场景、可信任、实战化”的智慧安全3.0安全理念，“全场景”把智慧安全的外延扩展到整个网络空间，全部数字化应用场景；“实战化”呼应当前新形势要求，而“可信任”的则是内涵的扩展，充分参考了CARTA及零信任模型，认为安全不仅仅是攻击防护，还是信任模型的建立与保障，通过持续验证多方身份、持续行为评估，摆脱传统的补丁式、外挂式、围墙式思路，形成网络安全纵深防御信任保障体系。

## 零信任架构

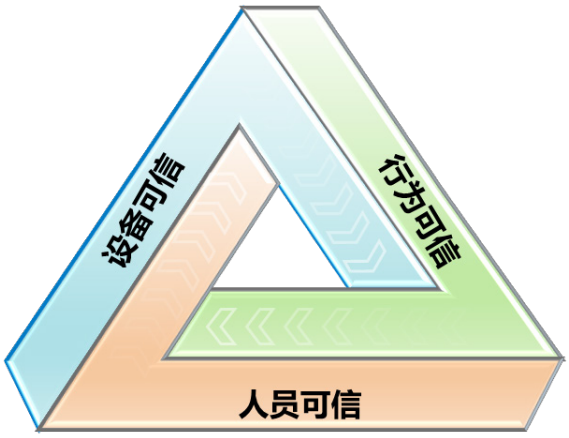
我们通过模拟黑客攻击来还原整个攻击链过程，以此来研究传统网络安全防护思路中的薄弱点及弱势。攻击者不管出于何种目的，在攻击行为发生时，一般都是通过网络边界漏洞、社工等手段获取用户身份，继而利用获取的合法身份通过终端登录目标系统、触发违规行为获取非法数据，以此来达成攻击目的。在这种传统的防御模式下，一旦攻击者突破了边界，利用非法获取到的合法身份，经过一次验证，安全措施就将形同虚设，进一步的横向攻击将不受阻碍。

这也是传统边界安全理念存在的先天不足，边界安全的建设其实已经默认了内网的安全性。边界一旦突破，内网就会被攻击者欲取予得。在这种传统边界理念先天劣势的状况下，零信任这种以资源保护为核心的网络安全范式，恰恰能够弥补边界安全思路的先天不足。既然网络访问的环节有不可信的风险，那么我们的管控手段就要覆盖到每个环节，对于任何用户、设备、行为默认都是不信任的，通过对身份、终端、行为多个角度持续评估信任关系，任意环节的失信都能通过策略联动，实现动态防护，持续保护内网资源安全。




## 可信访问三要素

网络安全能力的具体体现是为了保护内网资源的安全，用户对内网资源访问，实质上就是用户利用终端通过身份验证访问内网资源的行为。整个过程中为了保证业务访问通道的可信，通过智慧安全3.0可信任的理念，基于可信身份，可信设备，可信行为三方面，决定访问通道的建立，实现对客户业务环境的可信任访问。




**人员可信：**针对人员的可信体现在用户的身份认证和最小化权限授予。用户身份主要的目的是用于认证及授权，通常利用双因素认证或多因素认证的加强，通过短信、指纹、令牌多种认证方式建立一个多层次的身份验证层面的防御，如果一个认证因素遭到窃取，其他因素应该仍然存在，进而能够阻止非授权的访问。最小化权限授予，指的是人员在经过认证之后要实现对应用层面的最小授权，保证用户与应用的权限映射，只能获得完成任务的最小权限。

设备可信：终端设备是任何攻击发起的载体，为了更好的构建可信访问通道，我们将设备的身份、当前的安全状况等因素作为一个属性去判断访问通道是否可以建立。在访问建立之初，全面感知设备的当前安全性，终端安全防护的措施，以及安全基线情况，只有满足我们预先设置好的信任评估值，才能进行访问通道的建立。

**行为可信：**所有的访问意图都需要通过行为表达，为了确保访问行为的合规、可信，通过持续跟踪用户和终端发起的访问行为，这些行为可能是较长时间周期的异常行为，也可能是网络安全角度正常的违规行为，在传统的检测设备无法做出有效的响应的情况下，需要利用基线算法、图算法、时间序列分析等行为分析方法

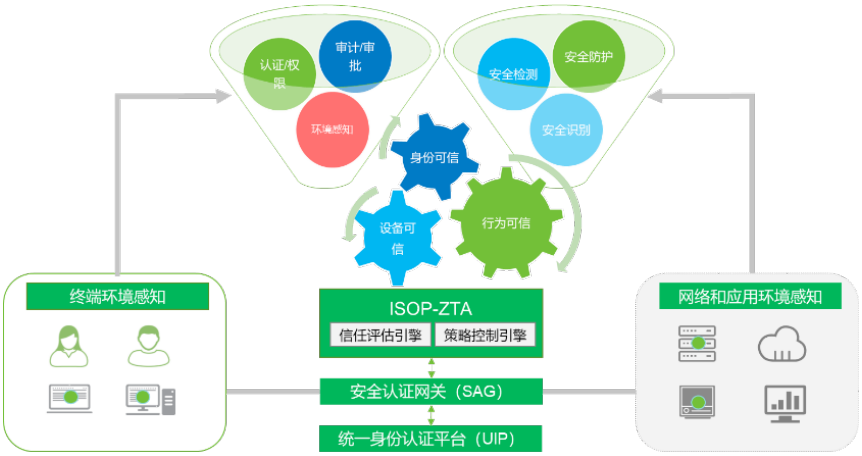
来做分析和检测。来发现内部威胁以及外部入侵行为。利用用户实体行为分析技术（UEBA）长周期分析用户行为特征，将行为特征进行横向与纵向对比，持续进行风险评估，更为全面地了解发现内部威胁以及外部入侵行为。

## 构建可信访问通道

网络安全最终的目的还是要应用于实战，强调更多的还是安全防护效果、安全措施的有效性，这些其实都需要实战化的演练进行验证。面对新的形势，安全已不仅是合规要求，安全融入业务，与业务共生、安全建设中也应与时俱进摒弃传统的边界安全思想，基于CARTA及零信任模型，最小化攻击暴露面，根据业务重要性重建可信访问通道。

在整个安全的业务访问通道建立过程中，整个访问通道通过零信任的安全部件，利用终端环境感知，实时感知设备安全状态，通过可信认证网关实现应用暴露面隐藏，通过统一身份管理平台来持续验证用户的身份和权限，验证终端设备的安全性。

可信访问的原则是单一因素的可信,并不能代表访问的可信, 需要多方面评估三者之间关系。通过零信任分析和控制平台将汇聚的数据结合资产组网、防护关系、历史行为数据、安全事件等各种数据，对用户、终端、应用、网络环境进行风险和信任分析，一旦某一个环节出现问题，通过自动化编排结合专家研判等方式,动态调整安全策略, 实现对风险的快速和自适应响应。




## 可信任、更安全

随着数字经济的深入发展，“数字信任”将会成为未来的一大热点。智慧安全3.0提出的“可信任”要素，突破了传统网络安全的界限，从业务视角出发，融入零信任思想，为用户构建信任模型，以应对复杂多变的网络环境与威胁。另一方面，持续保障自身安全能力、产品与服务的可信任，构建可信任网络环境，优化安全策略，形成对安全防御保障体系的持续优化，确保网络安全综合防护能力和水平的显著提升。

NSFOCUS

# 行业研究

# 《网络安全审查办法（修订草案征求意见稿）》解读

## 构建数据安全供需发展新格局

近日，国家互联网信息办公室（以下简称“网信办”）发布了《关于<网络安全审查办法（修订草案征求意见稿）>公开征求意见的通知》（以下简称《征求意见稿》），对《网络安全审查办法》内容提出了重要修订。从此次修订的变化，能够看出网络安全和数据安全发展情势的变化，也可读出其对数据安全政策和产业的影响。

## 一、内容修订情况：一条主线

此次《征求意见稿》相比之前的《网络安全审查办法》，其核心修订，也是最为重要的内容变化是加强了对数据安全的关注和规范。具体表现在以下三个方面。

**一是将数据安全法增加为立法依据。**《征求意见稿》第一条规定：“依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》，制定本办法”，将《中华人民共和国数据安全法》增加为制定依据，直接表明了本次修订的主旨就是通过网络安全审查制度、机制加强对数据安全相关行为的规范。这不仅仅是法规间衔接的要求，更是切实强化数据安全的必然举措。

**二是将数据处理活动作为重点规范对象。**《征求意见稿》第二条规定：“数

据处理者(以下称运营者)开展数据处理活动，影响或可能影响国家安全的，应当按照本办法进行网络安全审查”。可见，下一步《网络安全审查办法》的管理范围将有很大拓展，其在规范主体、规范行为两大方面都有扩大。结合近期国家主管部门先后宣布对多家互联网厂商进行审查的情况来看，办法修订生效后，也极有可能成为主管部门加强数据安全执法行动在操作层面的主要法律依据。

**三是对数据运营者作出了定量描述。**《征求意见稿》第六条规定：“掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查”。从该条规定可以看出，《征求意见稿》将掌握一定数量个人信息的企业赴国外上市，作为应当进行网络安全审查的一种数据处理行为，而且从相关修订条文比重来看，满足特定条件的国内企业赴国外上市很可能成为下一步网络安全审查的重点规范。

此外，《征求意见稿》还涉及到其他重要内容补充修订，如：将证监会增加进审查机制、审查提交材料增加了“拟提交的IPO材料”、特别审查程序由45天延长至3个月等。可见，这些修订内容，也均与数据安全的修订直接相关。

## 二、内容修订分析：三个要素

《征求意见稿》立足数据安全主线，其修订内容还充分反映了与数据安全存在密切关联的三个逻辑要素。

### （一）数据安全审查——明确机制

首先从法理上看，加强数据安全管理、完善数据安全审查机制是落实《数据安全法》的重要步骤。6月10日颁布的《数据安全法》即将于9月1日正式生效施行，此次《征求意见稿》将数据安全相关内容作为修订重点，无疑是数据安全法正式实施前的一项重要制度准备。《数据安全法》第二十四条明确规定：“国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查”，尽管此处的“国家安全审查”的方式和范围尚不得而知，但网络安全审查作为国家安全审查的重要组成部分应该是没有异议的。将数据安全纳入网络安全审查范畴，在具体操作中也符合管理效率原则和网络安全保障工作实情。

其次从数据安全的双重含义来看，在审查中不应偏废。理解数据安全应包含两层含义，一个是数据信息本身的安全属性要求，即通常所说的机密性、完

整性、可用性、真实性、可控性等属性，可称之为直接安全或内在安全；另一个是因对数据的不当处理行为而带来的安全风险，可以称之为间接安全或外在安全。《网络安全审查办法》此前对于第一种情形即数据的内在安全性已经作出了规定，如第九条第一款“产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险”。而此次《征求意见稿》对于数据安全的补充修订，很大程度上是对数据安全的第二层含义，即外在安全性的贯彻。可见，《征求意见稿》对数据安全进行的补充修订，其实质上是完善了数据安全的定义涵盖，而非无根据的随意扩展。因此从本质逻辑上看，数据安全的两个方面均是安全审查的重要对象，二者是一致的也是不可分割的。

### （二）国外上市——重要审查场景

从《征求意见稿》内容侧重上不难发现，国外上市是其明确列出的数据运营者所从事的、可能影响国家安全的一种主要行为。加强对特定企业赴国外上市的安全监管，不仅是为了落实《关于依法从严打击证券违法活动的意见》政策要求，更是为管控国外上市带来数据安全风险隐患的客观需要。

尽管对“国外上市”含义的具体界定还有待进一步明确，而仅从近期主管部门宣布启动的几起网络安全审查来看，企业在国外上市的行为，会极大加剧相关重要数据面临的安全风险、以及被政治化歪曲利用的可能。

以美国为例，目前美国证券交易相关的管理规定主要包括《塞班斯法案（Sarbanes-Oxley Act）》、《外国公司问责法案（Holding Foreign Companies Accountable Act）》等，其要求上市公司的核心披露义务主要涉及“财务和管理弱点报告”和“审计底稿”等。这些披露材料乍看似乎与事关安全的重要数据、核心数据等没有太直接的联系，深入分析则会发现，安全隐患主要来源于两个方面。一方面，要求披露的内容本身可能包含某些安全敏感数据，如“审计底稿”通常包括被审计对象的组织机构及管理人员结构、重要合同、董事会会议纪要等，其中可能会包含我国行业数据和消费者信息，能反映我国关键信息基础的运行等情况，若任由美国收集难免影响到我国家安全利益。另一方面，也是风险最大的情况，即在美上市的公司除了负担直接的信息披露义务之外，还有面临各种调查的潜在风险。美国建立了相对体系化的审查调查机制，主导部门包括商务部（贸易调查）、司法部（不正当竞争调查、海外反腐败调查、知识产权调查等）等，一旦上市公司被纳入相关的审查调查，其调查的内容范围就极有可能扩大，也就会加大相关重要数据暴露或被政治化歪曲等的风险。

### （三）个人信息——界定审查对象

《征求意见稿》对于数据安全的修订，还有很重要的一条线索就是个人信息保护。从字面上理解，似乎数据安全和个人信息保护的界线相对清晰，前者属于公法范畴，侧重保护公共利益；后者属于私法范畴，侧重保护个人隐私。但二者的密切联系也不容忽视。

首先，掌握个人信息的数量，将直接影响数据运营者的行为性质。正如前所述《征求意见稿》第六条规定了：“掌握超过100万用户个人信息的运营者赴国外上市”的时候，要必须向网络安全审查办公室申报网络安全审查。可见，按照《征求意见稿》该条内容理解，个人信息的定量情况将直接决定着数据运营者的海外上市行为是否影响国家安全，是判定数据运营者在海外上市能否触发网络安全审查的先决条件。

其次，个人信息在一定条件下，将直接转化为重要数据。因为二者在某些情况下存在一定的交集，如特定人物的个人信息、特定群体个人信息的汇聚等都有可能使个人信息转

化为重要或核心数据，这些数据因能够反映地区或行业、设施运行情况，从而必须纳入国家安全的视野范围加以保护。例如网络上曝光的对某些国家部委工作人员上下班出行情况的分析，这些出行信息具有很强的个人属性，本属于个人信息的范畴，但对这些信息进行汇聚和分类分析，就成了能够反映国家重要机构运行情况的数据，就不能再单纯视作个人信息了。在此意义上也可看出，个人信息与数据安全关系密不可分。

## 三、影响分析：构建数据安全供需发展新格局

当前“十四五”规划已经开局，将《征求意见稿》与即将生效的《数据安全法》结合起来并置于“十四五”新发展格局大背景中进行思考，对经济社会发展、产业提振将有更加实际的意义。“十四五”规划明确部署了新发展格局的实施路径：“把实施扩大内需战略同深化供给侧结构性改革有机结合起来，以创新驱动、高质量供给引领和创造新需求，加快构建以国内大循环为主体、国内国际双循环相互促进的新发展格局”，此次网络安全审查制度的修订，也将从供给、需求两个方面对数据安全发展带来积极影响，推动我国数据安全行业发展新格局的加速构建。

### （一）强化数据安全供给：技术创新、管理机制缺一不可

数据安全的供给侧主要偏重于构建数据安全保障能力，包括管理规范、技术手段、管理队伍等要素供给能力。

从管理规范供给能力看。一方面现有的数据安全管理法规政策之间将进一步衔接，从国家近期相继发布《关于依法从严打击证券违法活动的意见》（两办）、《征求意见稿》、《数字经济对外投资合作工作指引》（商务部、中央网信办、工信部联合印发）等重磅政策法规不难看出，数据安全与证券跨境监管、关键基础设施采购等的关系正在更加紧密地协同。另一方面，数据安全管理法规体系的健全工作将进一步提速，覆盖面也将逐步扩展，如关键基础设施数据处理活动风险评估管理、境外发行证券的保密和档案管理、跨境信息提供机制与流程管理、跨境审计监管合作等。

从技术手段供给能力来看。将有力促进数据安全相关技术产品和服务能力的创新发展，围绕不同层面需求，数据安全产品技术和服务供给能力将进一步深

化。在满足企事业单位自身数据安全保护需求方面，重点发展方向包括：数据防泄露、数据脱敏、数据库防火墙，以及以数据资产识别、管理为核心的数据安全管理平台等；在满足主管部门监管需求方面，重点发展方向包括：数据分级分类管理、敏感数据发现、数据安全风险评估、数据安全审计、数据追踪溯源等；在满足公共数据安全能力提升需求方面，重点发展方向包括：数据安全灾备、数据安全培训、数据安全运营等服务保障能力。

从管理队伍供给能力来看。数据安全在审查工作中的重要性日益增强，管理队伍的专业化水平将亟待同步提升。与之相适应的数据安全队伍供给体系重点方向将包括：数据安全类专业人才培养体系、选拔任用机制、培训实战体系、绩效考核机制等。

### （二）拓展数据安全需求：多管齐下应用引领

数据安全的需求侧主要偏重于建立数据安全应用体系，可归纳为三个“需求”：管理需求、合规需求和攻防需求。未来围绕数据安全需求的挖掘，不仅是主管部门引导数据安全健康有序发展的重要依据，也是深化数据安全技术创新和壮大数据安全产业能力的重要方向。

#### 1. 管理需求

对数据要做到“心中有数”。“底数不清”往往是出现数据安全问题的重要根源之一，明确数据安全管理需求的重点就是要做到对自身数据及其安全情况有较为清晰的了解。这类需求将主要围绕数据分类、数据分级、数据资产构成分析、数据防护现状分析等展开。

#### 2. 合规需求

数据安全应符合“法规红线”。网络安全等级保护、关键信息基础设施保护、保密管理等制度规范，对于数据都提出了相应的安全要求及相应防护手段。除了等保、关基、保密等传统合规要求之外，针对数据应用的重要典型场景，如工业数据、交通数据、能源数据等，也将成为法规关注的重点需求领域。

#### 3. 攻防需求

数据安全当满足“实战有效”。数据安全保障手段的最终目的是其能够化解潜在数据风险或有效防御数据攻击。在此类需求方面，除了事中防御和事后补救手段之外，事前的发现、检验需求将成为数据安全建设需求的重中之重，与之相对应的数据安全态势监测、数据安全仿真检测、数据安全保护实效检验等也将日益受到更多关注。

“东方欲晓，莫道君行早”。《征求意见稿》汇总各方面意见后的最终内容如何，仍需拭目以待。而其对于我国网络安全审查制度的完善、对于社会各界数据安全保护意识提升的影响已经显现并将持续，数据安全政策法规体系和数据安全技术产业也将以此为契机，迎来发展的新阶段。

# 打个样｜如何更好地践行《网络产品安全漏洞管理规定》？

## 推动网络产品安全漏洞管理工作的制度化、规范化、法治化

近日，工业和信息化部、国家互联网信息办公室、公安部近日联合印发《网络产品安全漏洞管理规定》（以下简称《规定》）。该《规定》的发布对于安全漏洞的发现、报告、修复、收集等多个行为进行了规范和约束，能够促使网络安全行业更快更健康的发展，同时也说明了国家对于网络安全的重视程度，强调了网络安全的发展和建设应以不损害国家安全为前提，绿盟科技基于网络安全攻防技术研究二十一年的经验，对如何更好地遵守并实践该《规定》整理了自己的理解以飨读者。

### 《规定》的法律依据

《网络安全法》中，对网络安全产品和网络运营者做了要求，这是《规定》制定依据，细化管理对象的规范要求。

**第二十二条** 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

**第二十五条** 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

### 《规定》管理对象

《规定》的管理对象包括：网络产品提供者、网络运营者、从事漏洞发现、收集、披露等活动的组织或个人。网络产品提供者和网络运营者是自身产品和系统漏洞的责任主体，需要建立畅通的漏洞信息接收渠道，及时对漏洞进行验证并完成漏洞修补。对于从事漏洞发现、收集、发布等活动的组织和个人，《规定》明确了其经评估协商后可提前披露产品漏洞、不得发布网络运营者漏洞细节、同步发布修补防范措施、不得将未公开漏洞提供给产品提供者之外的境外组织或者个人等八项具体要求。

## 绿盟科技的实践

绿盟科技八大实验室之一天机实验室，专注于漏洞挖掘和分析等攻防对抗的研究，同时，绿盟科技面向市场提供的60余款网络安全产品也经过高度严格的安全审查。此二者，都是《规定》中所提到的管理对象，需要满足《规定》之要求。绿盟科技对外发布的威胁信息一直坚持客观、真实、审慎、负责的原则，并且内部有一套成熟的情报生态体系做支撑。我们基于事件和情报的运营体系，以绿盟科技安全运营中心的专家团队为核心，集成了SOAR和威胁情报能力的集成平台，依托遍布全国的安全服务团队，为客户提供准确高效的情报和应急处置服务。

从绿盟科技内部的管理规定和日常要求出发，也制订并实施了一系列的工作制度与流程来满足《网络安全法》中对漏洞的要求，也契合《规定》中的细则。

首先，从网络产品提供者角度，绿盟科技成立了PSIRT（产品安全事件响应工作组）小组，专门负责产品安全漏洞的应急处置工作。覆盖公司交付客户的所有软件、硬件和在线服务产品。


图：绿盟科技产品漏洞应急处置流程

其次，绿盟科技制定《绿盟科技内部办公安全管理办法》，全员每年据此做个人安全等级的评测，包括实验室漏洞研究的同事在内的统一要求，明确测试授权、测试报备、测试过程等规定。

对于网站、软件/客户端/设备的扫描、渗透测试授权及漏洞通报，必须遵守以下规定:

A.严格禁止未经目标网站授权直接进行安全测试，以及各种途径的漏洞披露。B.对于客户授权我司对此客户负责或监管的网站/软件/客户端/设备进行的测试，应将测试结果直接通报客户项目联系人，禁止通报其他任何漏洞平台。

C.对于公开征集自身漏洞的网站或厂商，应将测试结果直接通报网站自身的漏洞上报平台。

D.对于通用软件/客户端/设备类对象的测试，应通过合法途径获得，并在本地实验环境下进行测试，测试结果直接通报高级安全研究部总监。

## 划个重点

《规定》面向网络产品安全漏洞的不同参与方提出了详细要求，需要大家引起重视：

### 针对网络产品提供者

1) 发现或获知漏洞后，应立即对漏洞进行验证、评估，并通报给存在漏洞的上游产品或组件提供者

2) 2日内将漏洞详情报送至工业和信息化部网络安全威胁和漏洞信息共享平台

3) 及时对漏洞进行修补，将漏洞风险、修补方式告知相关产品用户，并提供必要技术支持

4) 鼓励建立所提供网络产品安全漏洞的上报奖励机制

### 针对网络运营者

发现或者获知其运营网络产品安全漏洞后，应立即对漏洞进行验证并修补

针对网络产品漏洞发现、收集的组织和个人

1) 不得在网络产品提供者提供漏洞修补措施之前发布漏洞信息，提前发布需由工业和信息化部、公安部组织评估后进行

2) 不得发布网络运营者在用的网络产品漏洞细节

3) 不得刻意夸大漏洞危害和风险、实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动

4) 不得发布或提供专门用于利用漏洞从事危害网络安全活动的程序和工具

5) 在发布漏洞时，应同步发布修补或者防范措施

6) 国家重大活动期间，未经公安部同意，不得擅自发布漏洞信息

7) 不得将未公开漏洞信息向网络产品提供者之外的境外组织或者个人提供

### 针对网络产品安全漏洞收集平台

需在工业和信息化部备案，由工业和信息化部及时向公安部、国家互联网信息办公室通报，并对通过备案的漏洞收集平台予以公布。

以《网络安全法》为依据，《网络产品安全漏洞管理规定》将会推动网络产品安全漏洞管理工作的制度化、规范化、法治化，提高相关主体漏洞管理水平。绿盟科技携手业界同仁，发挥网络安全技术优势，学习和贯彻相关文件，为保障国家网络安全贡献力量。

# 攻防论道之保障篇｜克难制胜，攻防对抗之五步保障要领

## 绿盟科技五步保障法，战时防穿，突围不惧

张睿

随着网络安全成为国家战略，特别是《网络安全法》的正式颁布实施，网络安全建设正逐步走向实战化、体系化和常态化的新时代。在这一大背景下，攻防演练越来越受到各方重视，成为检验安全体系建设水平，促进安全运营能力提升的常备动作。

网络攻防演练保障工作不是一蹴而就，需要系统化的规划设计、统筹组织和部署执行。对于攻防演练的防御方，应按照启动阶段、备战阶段、临战阶段、保障阶段和总结阶段组织实施，不久前，绿盟君和大家就启动阶段、备战阶段、临战阶段分别需要注意问题以及应该部署的策略进行了论道，今天，我们来谈谈攻防演练的保障阶段需要如何排兵布阵。

当攻防对抗的大幕徐徐拉开，防守方面临着十面埋伏，危机重重。通过构建云地一体化联防联控安全保障体系，结合战时保障安全巡查、战时情报、安全保障中台协同联动机制，持续有效地进行威胁监控、分析研判、应急响应、溯源反制、事件上报网络攻防演练保障工作。


**全场景威胁监控：**实现本地内外网、云端全资产威胁联控，主、被动联合分层分特征异常发现，人员、资产、行为多重可信验证，情报、日志、全流量多特

征深度监测，生产与办公、业务与职能全场景覆盖；

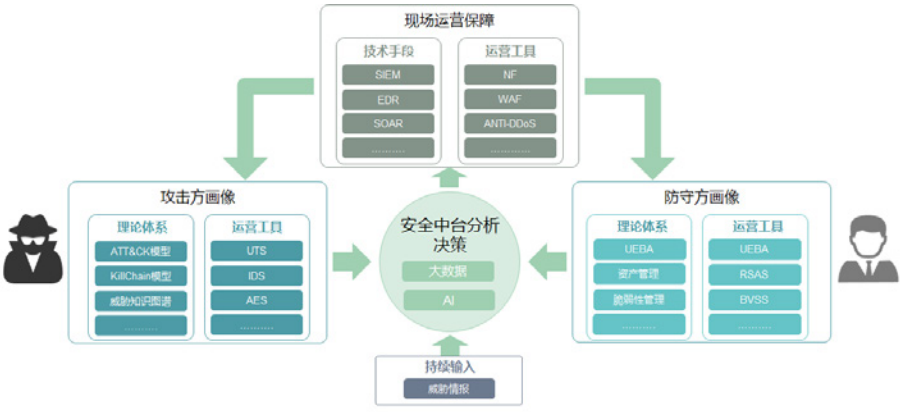
高效分析研判：多渠道汇集安全通告，线下结合线上、现场结合中台、情报结合狩猎，叠加多级网络安全专家研判体系，实现安全风险预警通告、安全事件应急通告、可疑安全行为通告迅速研判定性；

**应急响应处置：**应急前置预设流程全面高效启动，应急小组有条不紊分级分类处置安全事件，节奏化完成攻击阻断、取证备份、故障恢复、总结评估，双向联动全国跨地理、跨行业多维情报体系，多区域实时下发，技术策略实时滚动升级；

**威胁溯源反制：**一体化融合安全威胁检测设备、安全威胁分析平台、安全专家服务，整合平台监控、分析研判、中台应急能力，多技术手段溯源攻击方特性，遏制攻击扩散。锁定攻击源，针对性设计反制策略，多重诱捕，由点带面形成团队威慑力；

**高质量事件上报：**融合应急中台与情报滚动升级，持续强化一线作战研判水平与上报质量，分角色、分职能、分事件等级实现攻击取证、分析、研判过程记录，全面把控上报品质与上报效率，结合体系化得分点分析，确保防守团队成果可识别、可评价。

此外，依托绿盟科技在网络安全领域多年攻防实践经验，结合自身优势，充分整合研发、工程、对抗资源，拉通前后端能力，组建中台支撑体系，于实战保障期间，为一线团队提供有力支持，提供应急响应支撑和情报预警支撑保障。




严防守、重对抗、联动中台、协同保障，在没有硝烟的攻防对抗战场，绿盟科技五步保障法，全面助力客户临危不惧、突围不乱。垓下霸王不卸甲，反制克敌五步生。

# Android 银行木马 Toddler 针对欧洲银行用户开展攻击活动

【关键字】Android、Toddler木马、银行、僵尸网络

## 事件概述

研究人员发现了一种在欧洲肆虐传播的新型 Android 银行木马“Toddler”。Toddler又称为 TeaBot、Anatsa，主要针对西班牙、德国、瑞士、荷兰等地区进行攻击。该恶意软件在今年1月份由 Cleafy 披露，攻击了欧洲60家银行用户。Bitdefender 研究人员表示在今年6月份的时候，西班牙和意大利用户成为 Toddler 恶意软件的主要感染目标。PRODAFT 研究人员还称迄今为止，该恶意软件至少感染移动设备7,632 台，窃取凭据1,000多组。

## 技术详情

该恶意软件主要通过安装包程序和 Android 应用程序等传播媒介传播，然后在受害者主机与 C2 通信下载专门制作的虚假登录界面，然后将下载的钓鱼页面视图放置在目标应用程序之上，诱使受害者输入银行账号密码，窃取凭据。该恶意软件还会尝试窃取其他账户记录，并且具备键盘记录、截取屏幕截图、拦截两步验证 (2FA) 代码、短信拦截、C2 通信、接收命令和将受感染设备连接到僵尸网络的功能。

信息来源：https://www.prodaft.com/resource/detail/toddler-mobile-banking-botnet-analysis-report

# 美国橡树岭银行披露数据泄露事件

【关键字】银行、数据泄露

## 事件概述

近日，美国北卡罗来纳州橡树岭银行披露2021年4月26日至27日之间发生的数据泄露事件。此次攻击事件导致橡树岭银行的五家分行短暂关闭，部分客户的敏感数据信息遭到泄露。橡树岭银行在发现攻击者在未经授权访问其银行客户数据后，立即向美国联邦调查局报告事件并展开调查。

调查发现，攻击者在访问银行系统后可能窃取了部分客户的历史敏感数据，在2009年9月30日之前开设账户的客户敏感信息可能遭到泄露，这些泄露的信息可能包括社会安全号码、银行账号、出生日期和驾驶证号码等信息。橡树岭银行的五家分行虽然受此次攻击事件影响在4月下旬都关闭两天，但是其银行发言人表示在关闭期间，客户依然可以访问网上银行和手机银行，以及通过 ATM 进行存款和取款。该银行已于7月7日向受影响客户发送数据泄露事件通知，并向受影响的客户提供12个月的身份保护服务。

截至外媒发表报道之前，橡树岭银行发言人表示目前没有任何证据证明其客户信息被盗。

信息来源：https://www.wfmynews2.com/article/news/local/bank-of-oak-ridge-cyberattack/83-d1d540ba-c6fb-473e-99f1-417771b181e9

# 美国金融公司摩根士丹利遭到黑客攻击，发生数据泄漏

【关键字】跨国金融公司、攻击、数据泄露

## 事件概述

美国跨国金融公司摩根士丹利 (Morgan Stanley) 公司于7月2日发表通知称，由于攻击者入侵第三方供应商 Guidehouse 的 Accellion FTA 服务器，摩根士丹利客户敏感信息遭到泄露。第三方供应商于今年5月份通知摩根士丹利公司数据泄露事件，随后摩根士丹利公司向受影响的客户发送数据泄露通知。该银行表示由于第三方供应商遭到黑客攻击，摩根士丹利客户涉及 Guidehouse 拥有的文件及加密文件可能遭到泄露，泄露的数据还包含股票参与者姓名、地址、出生日期、社会安全号码、法人公司名称等信息。据称，虽然被盗文件以加密形式存储在受感染的 Guidehouse Accellion FTA 服务器上，但攻击者在攻击过程中还获得解密的密钥，可能存在加密信息泄露。但摩根士丹利称被盗信息并不包含可以访问摩根士丹利客户金融账户的账号密码等敏感信息。

信息来源：https://s3.documentcloud.org/documents/20985259/morgan-stanley-bc-20210702.pdf

# 比特币网站 Bitcoin.org 遭到 DDoS 攻击

【关键字】比特币、DDOS攻击、拒绝服务

## 事件概述

近日，用户名为 Cøbra 在 Twitter 上发表推文称，比特币网站 Bitcoin.org 遭受到大规模的 DDoS 攻击并被要求支付数额不详的比特币赎金。截至推文发表之前，该网站仍可被访问。该网站在去年 12 月成为类似 DDoS 攻击的目标，攻击导致用户在几小时内无法访问 Bitcoin Core 客户端。

全球性的加密货币交易所 Binance 称其去年的 DDoS 攻击是由竞争对手发起的，其主要目的是损耗声誉而不是窃取资金。DDoS 攻击往常主要针对加密货币交易所，但此次针对 Bitcoin.org 网站的 DDoS 攻击似乎不同寻常，因为该网站不包含有关资金或用户的敏感信息，只包含有关 BTC 区块链和加密货币的开源信息。

信息来源：https://twitter.com/CobraBitcoin/status/1412105666106478595

# 美国保险巨头 AJG 遭到勒索软件攻击，数据发生泄露

【关键字】保险公司、勒索软件、数据泄露

## 事件概述

近日，美国保险巨头 AJG 发布了关于勒索事件造成数据泄露的安全通知。AJG 称在去年9月份的时候检测到勒索软件的攻击活动，随即下线了所有系统，启动应急响应协议，向执法部门报告事件，并展开调查。调查发现，此次攻击活动始于2020年6月3日，攻击者可能在此期间内访问或窃取了部分敏感数据，但无法确认具体泄露了哪些信息。由于受影响的系统中存在社会安全号码、税号、护照、出生日期、用户名、密码、金融账户、信用卡信息、电子签名、医疗诊断、索赔等信息，AJG 表示受影响系统中的这些信息可能因此泄露。AJG 在检测到攻击后，当即向美国证券交易所报告了此次事件。目前，AJG 已就此次数据泄露信息事件，紧急通知数据监管当局和所有可能受到影响的客户。

AJG（Arthur J. Gallagher）是一家致力于全球保险经纪和风险管理的公司，其总部位于美国，业务遍及 49 个国家/地区。AJG 在 6 月 30 日的安全事件通知中表示会对此次泄露事件受影响的客户提供免费身份和信用监控服务。

信息来源：https://www.documentcloud.org/documents/7219617-AJG-BC-8-K.html

# ATM 缺陷：攻击者可以利用 NFC 和 Android 应用程序入侵 ATM

【关键字】ATM、NFC模块缺陷、Android应用程序、入侵、安装勒索软件

## 事件概述

ATM 网络攻击通常需要攻击者物理访问 USB 端口接入目标机器，而近日研究人员发现了 ATM 的一种缺陷，可以让攻击者直接利用 NFC 智能模块和 Android 应用程序入侵 ATM，不再需要物理访问方式接入受害者。据研究人员表示攻击者直接将专有的 Android 应用程序和具有 NFC 功能的智能手机一起使用，就可以轻松的在受害者设备上安装某种勒索软件，然后通过连接一台 ATM 计算机，攻击者就可以直接通过操作智能手机轻松窃取钱款。《连线》杂志报道称，这种攻击方式不仅可以入侵 ATM 自动取款机，还可以入侵其他自动售货机终端获取支付卡信息、感染恶意软件以及使 ATM 机中毒。由于研究人员和 ATM 供应商签订的保密协议，研究人员暂未透露关于此缺陷的更多细节。

信息来源：https://gbhackers.com/researcher-managed-to-hack-atms/

# Ursnif 和 Cerberus 针对意大利的在线银行用户开展攻击活动

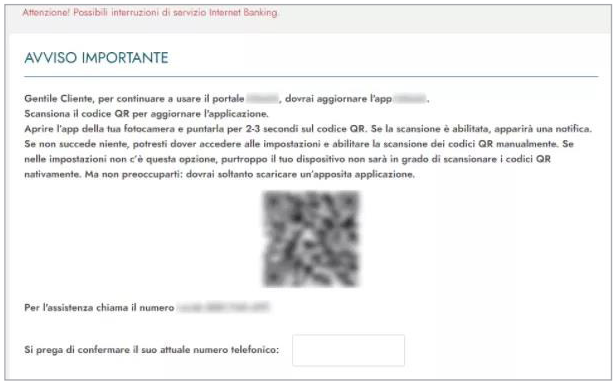
【关键字】银行木马、意大利在线银行、结合恶意软件、欺诈性转账

## 事件概述

IBM Trusteer 研究人员在一项针对银行行业的研究中发现 Ursnif（又名 Gozi） 银行木马被广泛用于攻击意大利在线银行用户。 恶意软件经销商将 Ursnif 银行木马与 Cerberus 恶意软件结合起来实现欺诈性银行转账的自动化。

攻击者不仅向受害者计算机投递含有附件的钓鱼邮件，使受害者桌面感染 Ursnif 恶意软件之外，还诱使受害者从虚假的 Google 商店下载移动应用程序，感染受害者的移动设备，并通过 Cerberus 恶意软件组件接收银行发送给客户的双因素身份验证代码，实时确认账户更新和汇款交易信息。

Cerberus 是一种覆盖类型的移动端恶意软件，于 2019 年中旬出现，具有劫持 SMS 内容、获取锁屏密码远程控制设备、数据窃取等功能。




信息来源：https://securityintelligence.com/posts/ursnif-cerberus-android-malware-bank-transfers-italy/

NSFOCUS

# 漏洞聚焦

# Linux 内核权限提升漏洞（CVE-2021-33909）

发布时间：2021-07-22

## 一、漏洞概述

近日，绿盟科技CERT监测发现Qualys研究团队披露了Linux 内核文件系统层中的一个本地提权漏洞（CVE-2021-33909，也称为Sequoia），该漏洞为Linux 内核的seq_file 接口存在size_t-to-int 类型转换漏洞，由于fs/seq_file.c 没有正确限制 seq 缓冲区分配，从而导致整数溢出、越界写入以及权限提升。任意用户权限的攻击者都可以在默认配置中利用此漏洞，从而获得受影响主机的root 权限。该漏洞影响了自 2014 年以来发布的所有 Linux 内核版本，目前PoC已公开，请相关用户尽快采取措施进行防护。

参考链接：

https://www.qualys.com/2021/07/20/cve-2021-33909/sequoia-local-privilege-escalation-linux.txt

## 二、影响范围

### 受影响版本

☐ 3.16 <= Linux kernel < 5.13.4

### 不受影响版本

☐ Linux kernel >= 5.13.4

## 三、漏洞检测

### 3.1 版本检测

Linux系统用户可以通过查看版本来判断当前系统是否在受影响范围内，查看操作系统版本信息命令如下：cat /proc/version

```
[root@test ~]# cat /proc/version
Linux version 3.10.0-514.26.2.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc
version 4.8.5 20150623 (Red Hat 4.8.5-11) (GCC) ) #1 SMP Tue Jul 4 15:04:05 UTC
2017
```

## 四、漏洞防护

### 4.1 官方升级

目前官方已在最新版本中修复了该漏洞，请受影响的用户尽快升级版本进行防护，官方下载链接： https://www.kernel.org/

### 4.2 临时缓解措施

若相关用户暂时无法进行升级操作，可针对Qualys已知的特定漏洞利用进行临时防护：

（1）将 /proc/sys/kernel/unprivileged_userns_clone设置为 0，以防止攻击者在用户命名空间中挂载长目录。

（2）将 /proc/sys/kernel/unprivileged_bpf_disabled 设置为 1，以防止攻击者将eBPF程序加载到内核中。

# Oracle 全系产品 7 月关键补丁更新通告

发布日期：2021-07-22

## 一、漏洞概述

2021年7月21日，绿盟科技CERT监测发现Oracle官方发布了7月关键补丁更新公告CPU（Critical Patch Update），共修复了342个不同程度的漏洞，此次安全更新涉及Oracle Database Server、Oracle Java SE、Oracle Fusion Middleware、Oracle MySQL、Oracle Communications等多个常用产品。Oracle强烈建议客户尽快应用关键补丁更新修复程序，对漏洞进行修复。

参考链接：

https://www.oracle.com/security-alerts/cpujul2021.html

## 二、重点漏洞简述

根据产品流行度和漏洞重要性筛选出此次更新中包含影响较大的漏洞，请相关用户重点进行关注：

Oracle MySQL多个漏洞：

此次安全更新针对Oracle MySQL发布了41个安全补丁, 有10个漏洞在未经用户身份验证的情况下即可远程进行利用。其中高危漏洞如下：

- ☐ CVE-2021-22884
- ☐ CVE-2021-22901

Oracle Communications Applications多个漏洞：

此次安全更新针对Oracle Communications Applications发布了33个安全补丁，有22个漏洞在未经用户身份验证的情况下即可远程进行利用。其中高危漏洞如下：

- ☐ CVE-2020-11612
- ☐ CVE-2021-3177
- ☐ CVE-2020-17530
- ☐ CVE-2019-17195
- ☐ CVE-2019-17195
- ☐ CVE-2020-11612
- ☐ CVE-2020-10878
- ☐ CVE-2020-14195

Oracle E-Business Suite多个漏洞：

此次安全更新针对Oracle E-Business Suite发布了17个安全补丁，有3个漏洞在未经用户身份验证的情况下即可远程进行利用。其中高危漏洞如下：

- ☐ CVE-2021-2355
- ☐ CVE-2021-2436
- ☐ CVE-2021-2359

Oracle Fusion Middleware多个漏洞：

此次安全更新针对Oracle Fusion Middleware发布了48个安全补丁，有35个漏洞在未经用户身份验证的情况下即可远程进行利用。其中高危漏洞如下：

- ☐ CVE-2021-2394
- ☐ CVE-2021-2397
- ☐ CVE-2021-2382
- ☐ CVE-2021-2456
- ☐ CVE-2019-17195
- ☐ CVE-2020-10683
- ☐ CVE-2020-28052

Oracle Retail Applications多个漏洞：

此次安全更新针对Oracle Retail Applications发布了23个安全补丁，有15个漏洞在未经用户身份验证的情况下即可远程进行利用。其中高危漏洞如下：

- ☐ CVE-2021-21345
- ☐ CVE-2019-0219

## 三、影响范围

Oracle官方7月关键补丁更新漏洞总结如下：

| 产品 | 漏洞个数 | 未授权远程利用个数 | 最高 CVSS 评分 |
|---|---|---|---|
| Oracle Database Products Risk Matrices | 16 | 1 | 8.3 |
| Oracle Database Server | 16 | 1 | 8.3 |
| Oracle Big Data Graph | 2 | 2 | 8.8 |
| Oracle Essbase | 9 | 8 | 10 |
| Oracle Commerce | 11 | 8 | 9.8 |
| Oracle Communications Applications | 33 | 22 | 9.9 |

| 产品 | 漏洞个数 | 未授权远程利用个数 | 最高 CVSS 评分 |
|---|---|---|---|
| Oracle Communications | 26 | 23 | 9.8 |
| Oracle Construction and Engineering | 10 | 5 | 9.8 |
| Oracle E-Business Suite | 17 | 3 | 9.1 |
| Oracle Enterprise Manager | 8 | 8 | 9.8 |
| Oracle Financial Services Applications | 22 | 17 | 9.9 |
| Oracle Food and Beverage Applications | 6 | 0 | 8.1 |
| Oracle Fusion Middleware | 48 | 35 | 9.9 |
| Oracle Hospitality Applications | 1 | 0 | 5.5 |
| Oracle Hyperion | 6 | 4 | 9.8 |
| Oracle Insurance Applications | 4 | 3 | 8.8 |
| Oracle Java SE | 6 | 5 | 9.8 |
| Oracle JD Edwards | 9 | 8 | 9.8 |
| Oracle MySQL | 41 | 10 | 8.8 |
| Oracle PeopleSoft | 14 | 8 | 9.8 |
| Oracle Policy Automation | 1 | 1 | 9.8 |
| Oracle Retail Applications | 23 | 15 | 9.9 |
| Oracle Siebel CRM | 6 | 4 | 8.1 |
| Oracle Supply Chain | 5 | 5 | 7.5 |
| Oracle Support Tools | 1 | 1 | 6.1 |
| Oracle Systems | 11 | 9 | 9.8 |
| Oracle Virtualization | 6 | 1 | 9.9 |
| Oracle Database Products Risk Matrices | 16 | 1 | 8.3 |
| Oracle Database Server | 16 | 1 | 8.3 |
| Oracle Big Data Graph | 2 | 2 | 8.8 |

| 产品 | 漏洞个数 | 未授权远程利用个数 | 最高 CVSS 评分 |
|---|---|---|---|
| Oracle Essbase | 9 | 8 | 10 |
| Oracle Commerce | 11 | 8 | 9.8 |
| Oracle Communications Applications | 33 | 22 | 9.9 |
| Oracle Communications | 26 | 23 | 9.8 |
| Oracle Construction and Engineering | 10 | 5 | 9.8 |
| Oracle E-Business Suite | 17 | 3 | 9.1 |
| Oracle Enterprise Manager | 8 | 8 | 9.8 |
| Oracle Financial Services Applications | 22 | 17 | 9.9 |
| Oracle Food and Beverage Applications | 6 | 0 | 8.1 |
| Oracle Fusion Middleware | 48 | 35 | 9.9 |
| Oracle Hospitality Applications | 1 | 0 | 5.5 |
| Oracle Hyperion | 6 | 4 | 9.8 |
| Oracle Insurance Applications | 4 | 3 | 8.8 |
| Oracle Java SE | 6 | 5 | 9.8 |
| Oracle JD Edwards | 9 | 8 | 9.8 |
| Oracle MySQL | 41 | 10 | 8.8 |
| Oracle PeopleSoft | 14 | 8 | 9.8 |
| Oracle Policy Automation | 1 | 1 | 9.8 |
| Oracle Retail Applications | 23 | 15 | 9.9 |
| Oracle Siebel CRM | 6 | 4 | 8.1 |
| Oracle Supply Chain | 5 | 5 | 7.5 |
| Oracle Support Tools | 1 | 1 | 6.1 |
| Oracle Systems | 11 | 9 | 9.8 |
| Oracle Virtualization | 6 | 1 | 9.9 |

## 四、漏洞防护

### 4.1 补丁更新

请用户参考本文附录“受影响产品及补丁信息”及时下载受影响产品更新补丁，并参照补丁安装包中的readme文件进行安装更新，以保证长期有效的防护。

注：Oracle官方补丁需要用户持有正版软件的许可账号，使用该账号登陆https://support.oracle.com后，可以下载最新补丁。

## 五、附录：受影响产品及补丁信息

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| Big Data Spatial and Graph, versions prior to 2.0, prior to 23.1 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Enterprise Manager Base Platform, version 13.4.0.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Essbase, version 21.2 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Essbase Analytic Provider Services, versions 11.1.2.4, 21.2 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions prior to XCP2400, prior to XCP3100 | https://support.oracle.com/rs?type=doc&id=2788472.1 |
| Hyperion Essbase Administration Services, versions 11.1.2.4, 21.2 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Hyperion Financial Reporting, versions 11.1.2.4, 11.2.5.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Hyperion Infrastructure Technology, versions 11.1.2.4, 11.2.5.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Identity Manager, versions 11.1.2.2.0, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3 | https://support.oracle.com/rs?type=doc&id=2783281.1 |
| JD Edwards EnterpriseOne Orchestrator, versions 9.2.5.3 and prior | https://support.oracle.com/rs?type=doc&id=2787996.1 |
| JD Edwards EnterpriseOne Tools, versions 9.2.5.3 and prior | https://support.oracle.com/rs?type=doc&id=2787996.1 |

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| MICROS Compact Workstation 3, version 310 | https://support.oracle.com/rs?type=doc&id=2758251.1 |
| MICROS ES400 Series, versions 400-410 | https://support.oracle.com/rs?type=doc&id=2758251.1 |
| MICROS Kitchen Display System Hardware, version 210 | https://support.oracle.com/rs?type=doc&id=2758251.1 |
| MICROS Workstation 5A, version 5A | https://support.oracle.com/rs?type=doc&id=2758251.1 |
| MICROS Workstation 6, versions 610-655 | https://support.oracle.com/rs?type=doc&id=2758251.1 |
| MySQL Cluster, versions 8.0.25 and prior | https://support.oracle.com/rs?type=doc&id=2787955.1 |
| MySQL Connectors, versions 8.0.23 and prior | https://support.oracle.com/rs?type=doc&id=2787955.1 |
| MySQL Enterprise Monitor, versions 8.0.23 and prior | https://support.oracle.com/rs?type=doc&id=2787955.1 |
| MySQL Server, versions 5.7.34 and prior, 8.0.25 and prior | https://support.oracle.com/rs?type=doc&id=2787955.1 |
| Oracle Access Manager, version 11.1.2.3.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Agile Engineering Data Management, version 6.2.1.0 | https://support.oracle.com/rs?type=doc&id=2787997.1 |
| Oracle Agile PLM, versions 9.3.3, 9.3.5, 9.3.6 | https://support.oracle.com/rs?type=doc&id=2787997.1 |
| Oracle Application Express, versions prior to 21.1.0.0.4 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Application Express (CKEditor), versions prior to 21.1.0.0.1 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Application Express Application Builder (DOMPurify), versions prior to 21.1.0.0.1 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Application Testing Suite, version 13.3.0.1 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle BAM (Business Activity Monitoring), versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Banking Enterprise Default Management, versions 2.10.0, 2.12.0 | https://support.oracle.com/rs?type=doc&id=2787695.1 |
| Oracle Banking Liquidity Management, versions 14.2, 14.3, 14.5 | https://support.oracle.com |
| Oracle Banking Party Management, version 2.7.0 | https://support.oracle.com/rs?type=doc&id=2787695.1 |
| Oracle Banking Platform, versions 2.4.0, 2.7.1, 2.9.0, 2.12.0 | https://support.oracle.com/rs?type=doc&id=2787695.1 |

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| Oracle Banking Treasury Management, version 14.4 | https://support.oracle.com |
| Oracle BI Publisher, versions 5.5.0.0.0, 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Business Intelligence Enterprise Edition, version 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Coherence, versions 3.7.1.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Commerce Guided Search, version 11.3.2 | https://support.oracle.com/rs?type=doc&id=2792990.1 |
| Oracle Commerce Guided Search / Oracle Commerce Experience Manager, versions 11.3.1.5, 11.3.2 | https://support.oracle.com/rs?type=doc&id=2792990.1 |
| Oracle Commerce Merchandising, versions 11.1.0, 11.2.0, 11.3.0-11.3.2 | https://support.oracle.com/rs?type=doc&id=2792990.1 |
| Oracle Commerce Platform, versions 11.0.0, 11.1.0, 11.2.0, 11.3.0-11.3.2 | https://support.oracle.com/rs?type=doc&id=2792990.1 |
| Oracle Commerce Service Center, versions 11.0.0, 11.1.0, 11.2.0, 11.3.0-11.3.2 | https://support.oracle.com/rs?type=doc&id=2792990.1 |
| Oracle Communications Application Session Controller, version 3.9 | https://support.oracle.com/rs?type=doc&id=2787241.1 |
| Oracle Communications Billing and Revenue Management, versions 7.5.0.23.0, 12.0.0.3.0 | https://support.oracle.com/rs?type=doc&id=2785183.1 |
| Oracle Communications BRM - Elastic Charging Engine, versions 11.3.0.9.0, 12.0.0.3.0 | https://support.oracle.com/rs?type=doc&id=2785183.1 |
| Oracle Communications Cloud Native Core Console, version 1.4.0 | https://support.oracle.com/rs?type=doc&id=2791671.1 |
| Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.4.0, 1.7.0 | https://support.oracle.com/rs?type=doc&id=2791656.1 |
| Oracle Communications Cloud Native Core Network Slice Selection Function, version 1.2.1 | https://support.oracle.com/rs?type=doc&id=2791657.1 |

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| Oracle Communications Cloud Native Core Policy, versions 1.5.0, 1.9.0 | https://support.oracle.com/rs?type=doc&id=2791658.1 |
| Oracle Communications Cloud Native Core Security Edge Protection Proxy, version 1.7.0 | https://support.oracle.com/rs?type=doc&id=2791680.1 |
| Oracle Communications Cloud Native Core Service Communication Proxy, version 1.5.2 | https://support.oracle.com/rs?type=doc&id=2791682.1 |
| Oracle Communications Cloud Native Core Unified Data Repository, versions 1.4.0, 1.6.0 | https://support.oracle.com/rs?type=doc&id=2791683.1 |
| Oracle Communications Convergent Charging Controller, version 12.0.4.0.0 | https://support.oracle.com/rs?type=doc&id=2790722.1 |
| Oracle Communications Design Studio, version 7.4.2 | https://support.oracle.com/rs?type=doc&id=2789906.1 |
| Oracle Communications Diameter Signaling Router (DSR), versions 8.0.0-8.5.0 | https://support.oracle.com/rs?type=doc&id=2787208.1 |
| Oracle Communications EAGLE Software, versions 46.6.0-46.8.2 | https://support.oracle.com/rs?type=doc&id=2787243.1 |
| Oracle Communications Evolved Communications Application Server, version 7.1 | https://support.oracle.com/rs?type=doc&id=2787205.1 |
| Oracle Communications Instant Messaging Server, version 10.0.1.4.0 | https://support.oracle.com/rs?type=doc&id=2786444.1 |
| Oracle Communications Network Charging and Control, versions 6.0.1.0, 12.0.1.0-12.0.4.0, 12.0.4.0.0 | https://support.oracle.com/rs?type=doc&id=2790722.1 |
| Oracle Communications Offline Mediation Controller, version 12.0.0.3.0 | https://support.oracle.com/rs?type=doc&id=2785182.1 |
| Oracle Communications Pricing Design Center, version 12.0.0.3.0 | https://support.oracle.com/rs?type=doc&id=2785183.1 |
| Oracle Communications Services Gatekeeper, versions 7.0, 8.2 | https://support.oracle.com/rs?type=doc&id=2787242.1 |
| Oracle Communications Unified Inventory Management, versions 7.3.2, 7.3.4, 7.3.5, 7.4.0, 7.4.1 | https://support.oracle.com/rs?type=doc&id=27851890.1 |

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| Oracle Configuration Manager, version 12.1.2.0.8 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Data Integrator, versions 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Database Server, versions 12.1.0.2, 12.2.0.1, 19c | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle E-Business Suite, versions 12.1.1-12.1.3, 12.2.3-12.2.10 | https://support.oracle.com/rs?type=doc&id=2770321.1 |
| Oracle Enterprise Data Quality, versions 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Enterprise Repository, version 11.1.1.7.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6-8.0.9, 8.1.0 | https://support.oracle.com/rs?type=doc&id=2787723.1 |
| Oracle Financial Services Crime and Compliance Investigation Hub, version 20.1.2 | https://support.oracle.com/rs?type=doc&id=2792414.1 |
| Oracle Financial Services Regulatory Reporting with AgileREPORTER, version 8.0.9.6.3 | https://support.oracle.com/rs?type=doc&id=2791194.1 |
| Oracle Financial Services Revenue Management and Billing Analytics, versions 2.7.0, 2.8.0 | https://support.oracle.com/rs?type=doc&id=2787723.1 |
| Oracle FLEXCUBE Private Banking, versions 12.0.0, 12.1.0 | https://support.oracle.com |
| Oracle FLEXCUBE Universal Banking, versions 12.0-12.4, 14.0-14.4.0 | https://support.oracle.com |
| Oracle Fusion Middleware MapViewer, version 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle GoldenGate Application Adapters, version 19.1.0.0.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle GraalVM Enterprise Edition, versions 20.3.2, 21.1.0 | https://support.oracle.com/rs?type=doc&id=2787003.1 |
| Oracle Hospitality Reporting and Analytics, version 9.1.0 | https://support.oracle.com/rs?type=doc&id=2780088.1 |
| Oracle Hospitality Suite8, versions 8.13, 8.14 | https://support.oracle.com/rs?type=doc&id=2785669.1 |
| Oracle Hyperion BI+, versions 11.1.2.4, 11.2.5.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Insurance Policy Administration, versions 11.0.2, 11.1.0-11.3.0 | https://support.oracle.com/rs?type=doc&id=2784893.1 |
| Oracle Insurance Policy Administration J2EE, version 11.0.2 | https://support.oracle.com/rs?type=doc&id=2784893.1 |

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| Oracle Insurance Rules Palette, versions 11.0.2, 11.1.0-11.3.0 | https://support.oracle.com/rs?type=doc&id=2784893.1 |
| Oracle Java SE, versions 7u301, 8u291, 11.0.11, 16.0.1 | https://support.oracle.com/rs?type=doc&id=2787003.1 |
| Oracle JDeveloper, versions 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle JDeveloper and ADF, version 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Outside In Technology, version 8.5.5 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle Policy Automation, versions 12.2.0-12.2.22 | https://support.oracle.com/rs?type=doc&id=2782105.1 |
| Oracle Retail Back Office, version 14.1 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Central Office, version 14.1 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Customer Engagement, versions 16.0-19.0 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Customer Management and Segmentation Foundation, versions 16.0-19.0 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.3.0 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.3.0 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Merchandising System, versions 14.1.3.2, 15.0.3.1, 16.0.3 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Order Broker, versions 15.0, 16.0 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Order Management System Cloud Service, version 19.5 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Point-of-Service, version 14.1 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Price Management, versions 14.0, 14.1, 15.0, 16.0 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Returns Management, version 14.1 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.3.0 | https://support.oracle.com/rs?type=doc&id=2783353.1 |

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| Oracle Retail Xstore Point of Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1 | https://support.oracle.com/rs?type=doc&id=2783353.1 |
| Oracle SD-WAN Aware, versions 8.2, 9.0 | https://support.oracle.com/rs?type=doc&id=2787244.1 |
| Oracle SD-WAN Edge, versions 8.2, 9.0, 9.1 | https://support.oracle.com/rs?type=doc&id=2787240.1 |
| Oracle Secure Global Desktop, version 5.6 | https://support.oracle.com/rs?type=doc&id=2788251.1 |
| Oracle Solaris, version 11 | https://support.oracle.com/rs?type=doc&id=2788472.1 |
| Oracle Solaris Cluster, version 4.4 | https://support.oracle.com/rs?type=doc&id=2788472.1 |
| Oracle Transportation Management, version 6.4.3 | https://support.oracle.com/rs?type=doc&id=2787997.1 |
| Oracle VM VirtualBox, versions prior to 6.1.24 | https://support.oracle.com/rs?type=doc&id=2788251.1 |
| Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle WebLogic Server, versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Oracle ZFS Storage Appliance Kit, version 8.8 | https://support.oracle.com/rs?type=doc&id=2788472.1 |
| OSS Support Tools, versions prior to 2.12.41 | https://support.oracle.com/rs?type=doc&id=2787969.1 |
| PeopleSoft Enterprise CS Campus Community, versions 9.0, 9.2 | https://support.oracle.com/rs?type=doc&id=2787995.1 |
| PeopleSoft Enterprise HCM Candidate Gateway, version 9.2 | https://support.oracle.com/rs?type=doc&id=2787995.1 |
| PeopleSoft Enterprise HCM Shared Components, version 9.2 | https://support.oracle.com/rs?type=doc&id=2787995.1 |
| PeopleSoft Enterprise PeopleTools, versions 8.57, 8.58, 8.58.8.59, 8.59 | https://support.oracle.com/rs?type=doc&id=2787995.1 |
| PeopleSoft Enterprise PT PeopleTools, versions 8.57, 8.58, 8.59 | https://support.oracle.com/rs?type=doc&id=2787995.1 |
| Primavera Gateway, versions 17.12.0-17.12.11, 18.8.0-18.8.11, 19.12.0-19.12.10, 20.12.0 | https://support.oracle.com/rs?type=doc&id=2783281.1 |
| Primavera P6 Enterprise Project Portfolio Management, versions 17.12.0-17.12.20, 18.8.0-18.8.23, 19.12.0-19.12.14, 20.12.0-20.12.3 | https://support.oracle.com/rs?type=doc&id=2783281.1 |

| 受影响产品及版本号 | 可用补丁 |
| --- | --- |
| Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12 | https://support.oracle.com/rs?type=doc&id=2783281.1 |
| Real-Time Decisions (RTD) Solutions, version 3.2.0.0 | https://support.oracle.com/rs?type=doc&id=2773670.1 |
| Siebel Applications, versions 21.5 and prior | https://support.oracle.com/rs?type=doc&id=2787996.1 |
| StorageTek Tape Analytics SW Tool, version 2.3 | https://support.oracle.com/rs?type=doc&id=2788472.1 |

## 声明

# WebLogic 多个高危漏洞

发布日期：2021-07-22

## 一、漏洞概述

7月21日，绿盟科技CERT监测到Oracle官方发布了2021年7月关键补丁更新公告CPU（Critical Patch Update），共修复了342个不同程度的漏洞，其中包括3个影响WebLogic的严重漏洞，利用复杂度低，建议用户尽快采取措施，对此次的漏洞进行防护。

CVE-2021-2382/CVE-2021-2394/CVE-2021-2397：未经身份验证的攻击者发送恶意构造的T3或IIOP协议请求，可在目标服务器上执行任意代码，CVSS评分为9.8

CVE-2021-2376/CVE-2021-2378：未经身份验证的攻击者通过T3或IIOP协议发送恶意请求，可造成目标服务器挂起或崩溃，CVSS评分为7.5

CVE-2015-0254：此漏洞存在于Apache Standard Taglibs中，当应用程序使用 <x:parse> 或 <x:transform> 标签处理不受信任的XML文档时，1.2.3版本之前的 Apache Standard Taglibs允许远程攻击者利用XSLT 扩展执行任意代码或进行XML外部实体注入(XXE) 攻击，CVSS评分为7.3

CVE-2021-2403：未经身份验证的攻击者可以通过HTTP发送恶意请求，未授权访问目标服务器的某些数据，CVSS评分为5.3

参考链接：

https://www.oracle.com/security-alerts/cpujul2021.html#AppendixFMW

## 二、影响范围

**受影响版本**

- ☐ WebLogic Server 10.3.6.0.0
- ☐ WebLogic Server 12.1.3.0.0
- ☐ WebLogic Server 12.2.1.3.0
- ☐ WebLogic Server 12.2.1.4.0
- ☐ WebLogic Server 14.1.1.0.0

## 三、漏洞检测

### 3.1 本地检测

可使用如下命令对WebLogic版本和补丁安装的情况进行排查。

```
$ cd /Oracle/Middleware/wlserver_10.3/server/lib
$ java -cp weblogic.jar weblogic.version
```

在显示结果中，如果没有补丁安装的信息，则说明存在风险，如下图所示：

```
[root007@localhost lib]$ java -cp weblogic.jar weblogic.version

WebLogic Server 10.3.6.0  Tue Nov 15 08:52:36 PST 2011 1441050

Use 'weblogic.version -verbose' to get subsystem information

Use 'weblogic.utils.Versions' to get version information for all modules
[root007@localhost lib]$
```

### 3.2 T3协议探测

Nmap工具提供了WebLogic T3协议的扫描脚本，可探测开启T3服务的WebLogic主机。命令如下：

nmap -n -v -Pn  -sV [主机或网段地址] -p（默认）7001,7002 --script=weblogic-t3-info.nse

如下图红框所示，目标开启了T3协议且WebLogic版本在受影响范围之内，如果相关人员没有安装官方的安全补丁，则存在漏洞风险。

```
root@kali:~# nmap -v 172.16.1.128 -p7001,7002 --script=weblogic-t3-info.ns

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-19 19:07 CST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:07
Completed NSE at 19:07, 0.00s elapsed
Initiating ARP Ping Scan at 19:07
Scanning 172.16.1.128 [1 port]
Completed ARP Ping Scan at 19:07, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:07
Completed Parallel DNS resolution of 1 host. at 19:07, 0.02s elapsed
Initiating SYN Stealth Scan at 19:07
Scanning 172.16.1.128 [2 ports]
Discovered open port 7002/tcp on 172.16.1.128
Discovered open port 7001/tcp on 172.16.1.128
Completed SYN Stealth Scan at 19:07, 0.05s elapsed (2 total ports)
NSE: Script scanning 172.16.1.128.
Initiating NSE at 19:07
Completed NSE at 19:07, 4.90s elapsed
Nmap scan report for 172.16.1.128
Host is up (0.00061s latency).

PORT     STATE SERVICE
7001/tcp open  afs3-callback
| weblogic-t3-info: T3 protocol in use (WebLogic version: 10.3.6.0)
7002/tcp open  afs3-prserver
MAC Address: 00:0C:29:4C:79:FC (VMware)

NSE: Script Post-scanning.
Initiating NSE at 19:07
Completed NSE at 19:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.59 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
root@kali:~#
```

# 四、漏洞防护

## 4.1 补丁更新

目前Oracle已发布补丁修复了上述漏洞，请用户参考官方通告及时下载受影响产品更新补丁，并参照补丁安装包中的readme文件进行安装更新，以保证长期有效的防护。

注：Oracle官方补丁需要用户持有正版软件的许可账号，使用该账号登陆https://support.oracle.com后，可以下载最新补丁。

## 4.2 临时防护措施

如果用户暂时无法安装更新补丁，可通过下列措施对高危漏洞进行临时防护：

### 4.2.1 限制 T3 协议访问

用户可通过控制T3协议的访问来临时阻断针对利用T3协议漏洞的攻击。WebLogic Server提供了名为 weblogic.security.net.ConnectionFilterImpl 的默认连接筛选器，此连接筛选器接受所有传入连接，可通过此连接筛选器配置规则，对T3及T3s协议进行访问控制，详细操作步骤如下：

1、进入WebLogic控制台，在base_domain的配置页面中，进入“安全”选项卡页面，点击“筛选器”，进入连接筛选器配置。

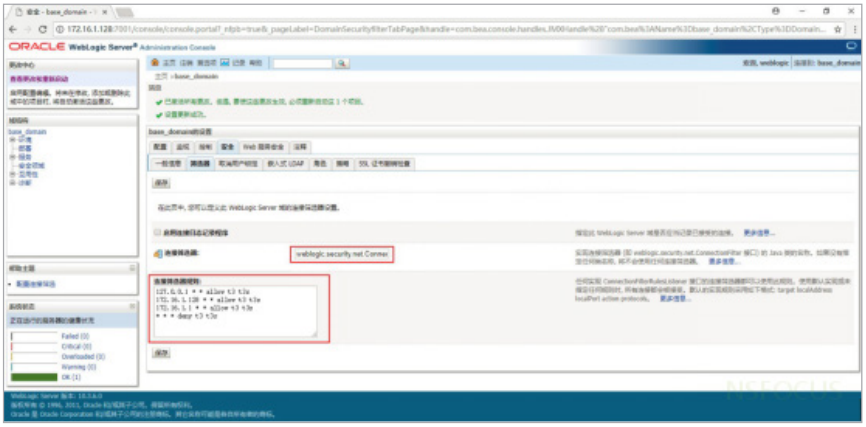

2、在连接筛选器中输入：weblogic.security.net.ConnectionFilterImpl，参考以下写法，在连接筛选器规则中配置符合企业实际情况的规则：

127.0.0.1 * * allow t3 t3s

本机IP ** allow t3 t3s

允许访问的IP * * allow t3 t3s

* * * deny t3 t3s



连接筛选器规则格式如下：target localAddress localPort action protocols，

其中：

target 指定一个或多个要筛选的服务器。

localAddress 可定义服务器的主机地址。(如果指定为一个星号 (*)，则返回的匹配结果将是所有本地 IP 地址。)

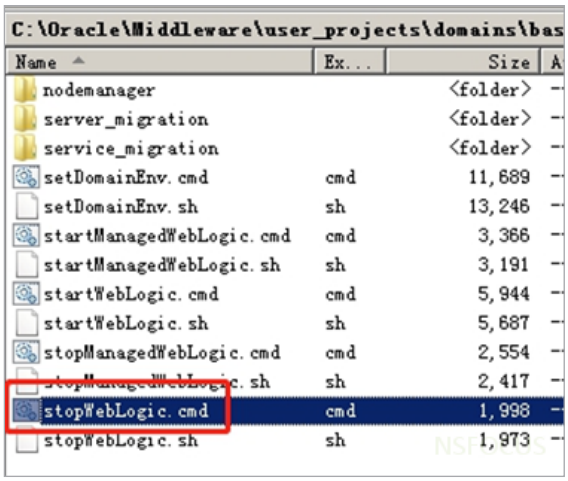
localPort 定义服务器正在监听的端口。(如果指定了星号，则匹配返回的结果将是服务器上所有可用的端口)。

action 指定要执行的操作。(值必须为“allow”或“deny”。)

protocols 是要进行匹配的协议名列表。(必须指定下列其中一个协议：http、https、t3、t3s、giop、giops、dcom 或 ftp。) 如果未定义协议，则所有协议都将与一个规则匹配。

3、保存后若规则未生效，建议重新启动WebLogic服务（重启WebLogic服务会导致业务中断，建议相关人员评估风险后，再进行操作）。以Windows环境为例，重启服务的步骤如下：

进入域所在目录下的bin目录，在Windows系统中运行stopWebLogic.cmd文件终止WebLogic服务，Linux系统中则运行stopWebLogic.sh文件。




待终止脚本执行完成后，再运行startWebLogic.cmd或startWebLogic.sh文件启动WebLogic，即可完成WebLogic服务重启。

### 4.2.2 禁用 IIOP 协议

用户可通过关闭IIOP协议阻断针对利用IIOP协议漏洞的攻击，操作如下：

在WebLogic控制台中，选择“服务”->“AdminServer”->“协议”，取消“启用IIOP”的勾选。并重启WebLogic项目，使配置生效。


## 声明

本安全公告仅用来描述可能存在的安全问题，绿盟科技不为此安全公告提供任何保证或承诺。由于传播、利用此安全公告所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，绿盟科技以及安全公告作者不为此承担任何责任。绿盟科技拥有对此安全公告的修改和解释权。如欲转载或传播此安全公告，必须保证此安全公告的完整性，包括版权声明等全部内容。未经绿盟科技允许，不得任意修改或者增减此安全公告内容，不得以任何方式将其用于商业目的。

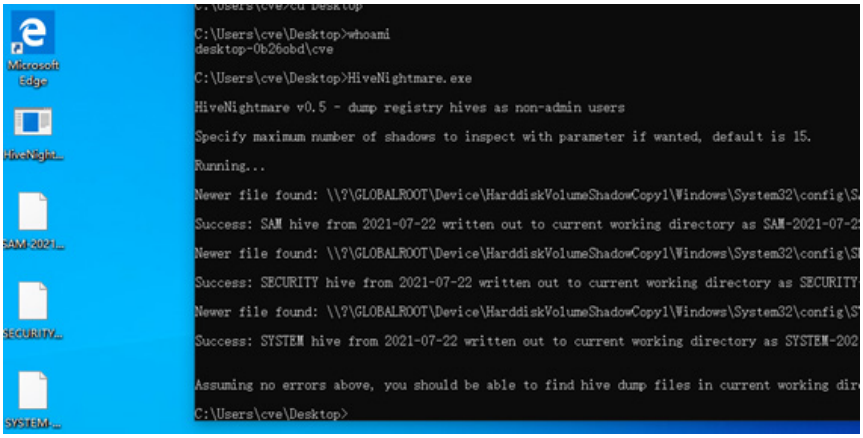
# WINDOWS 权限提升漏洞（CVE-2021-36934）通告

发布日期：2021-07-22

## 一、漏洞概述

近日，绿盟科技CERT监测到微软发布紧急通告，披露了Windows权限提升漏洞（CVE-2021-36934）。由于对多个系统文件（包括安全帐户管理器 (SAM) 数据库）的访问控制列表 (ACL) 过于宽松，当系统启用了内置管理员账户(administrator)时，普通用户可以利用此漏洞结合哈希传递攻击实现权限提升，从而在目标主机上以SYSTEM权限执行任意代码。目前漏洞细节与利用程序已公开，建议相关用户进行排查并采取措施进行防护。

绿盟科技CERT已成功复现此漏洞：




参考链接：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934

## 二、影响范围

**受影响版本**

- ☐ Windows Server, version 20H2 (Server Core Installation)
- ☐ Windows Server, version 2004 (Server Core installation)
- ☐ Windows Server 2019 (Server Core installation)
- ☐ Windows Server 2019
- ☐ Windows 10 Version 21H1 for x64-based Systems
- ☐ Windows 10 Version 21H1 for ARM64-based Systems
- ☐ Windows 10 Version 21H1 for 32-bit Systems

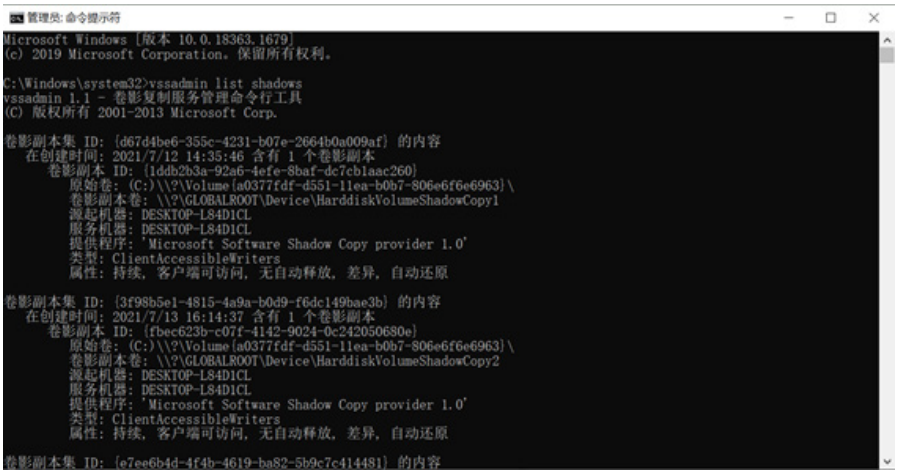
- ☐ Windows 10 Version 20H2 for x64-based Systems
- ☐ Windows 10 Version 20H2 for ARM64-based Systems
- ☐ Windows 10 Version 20H2 for 32-bit Systems
- ☐ Windows 10 Version 2004 for x64-based Systems
- ☐ Windows 10 Version 2004 for ARM64-based Systems
- ☐ Windows 10 Version 2004 for 32-bit Systems
- ☐ Windows 10 Version 1909 for x64-based Systems
- ☐ Windows 10 Version 1909 for ARM64-based Systems
- ☐ Windows 10 Version 1909 for 32-bit Systems
- ☐ Windows 10 Version 1809 for x64-based Systems
- ☐ Windows 10 Version 1809 for ARM64-based Systems
- ☐ Windows 10 Version 1809 for 32-bit Systems

## 三、漏洞检测

### 3.1 人工检测

系统版本在影响范围的用户可使用管理员权限运行下列命令查看VSS卷影进行排查：

vssadmin list shadows




若启用了系统保护且创建了系统还原点（大于128G的系统驱动盘执行Windows更新或安装 MSI默认创建VSS卷影副本），则受此漏洞影响。

## 四、漏洞防护

### 4.1 防护措施

目前官方暂未发布修复补丁，受影响用户可通过下列措施进行临时防护：

1、限制对 %windir%\system32\config 内容的访问

以管理员身份运行命令提示符执行下列命令：

icacls %windir%\system32\config*.* /inheritance:e

或以管理员身份运行PowerShell执行下列命令：

icacls $env:windir\system32\config*.* /inheritance:e

2、删除卷影复制服务 (VSS) 卷影副本

删除限制访问 %windir%\system32\config 之前存在的全部系统还原点和卷影（如需要可创建新的系统还原点）。

3、在不影响正常功能的前提下，可禁用内置管理员账户。

注意：以上删除卷影副本的缓解措施可能会影响还原操作，包括使用第三方备份应用程序还原数据的能力。但必须限制访问并删除卷影副本才能防止利用此漏洞。

# 微软 7 月安全更新多个产品高危漏洞通告

发布日期：2021-07-14

## 一、漏洞概述

7 月 14 日，绿盟科技 CERT 监测到微软发布 7 月安全更新补丁，修复了 117 个安全漏洞，涉及 Windows、Microsoft Office、Microsoft Edge、Visual Studio 、SharePoint Server 等广泛使用的产品，其中包括远程代码执行和权限提升等高危漏洞类型。

本月微软月度更新修复的漏洞中，严重程度为关键（Critical）的漏洞有 13 个，重要（Important）漏洞有 103 个。其中有 9 个为 0day 漏洞，有 5 个信息已被公开披露：

Windows 证书欺骗漏洞（CVE-2021-34492）

Microsoft Exchange Server 远程代码执行漏洞（CVE-2021-34473）Microsoft Exchange Server 权限提升漏洞（CVE-2021-34523）Windows ADFS 安全功能绕过漏洞（CVE-2021-33779）

Active Directory 安全功能绕过漏洞（CVE-2021-33781）有 4 个已被在野利用：

Windows Print Spooler 远程代码执行漏洞（CVE-2021-34527）Windows Script Engine 内存损坏漏洞（CVE-2021-34448） Windows Kernel 权限提升漏洞（CVE-2021-31979）

Windows Kernel 权限提升漏洞（CVE-2021-33771）

请相关用户尽快更新补丁进行防护，完整漏洞列表请参考附录。

绿盟远程安全评估系统（RSAS）已具备微软此次补丁更新中大多数漏洞的检测能力（包括 CVE-2021-34448、CVE-2021-34473、CVE-2021-34494、CVE-2021-34458、CVE-2021-34527 等高危漏洞），请相关用户关注绿盟远程安全评估系统系统插件升级包的更新，及时升级至 V6. 0R02F01.2401，官网链接：http://update.nsfocus.com/update/listRsasDetail/v/vulsys

参考链接：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Jul

## 二、重点漏洞简述

根据产品流行度和漏洞重要性筛选出此次更新中包含影响较大的漏洞，请相关用户重点 进行关注：

Windows Print Spooler 远程代码执行漏洞（CVE-2021-34527）：

Print Spooler 是 Windows 系统中管理打印相关事务的服务，域用户可远程利用该漏洞以 S YSTEM 权限在域控制器上执行任意代码，从而获得整个域的控制权。此漏洞 EXP 已公开且被在野利用，绿盟科技 CERT 全程追踪了此漏洞，详情及防护措施请参考：https://mp.weixin.qq. com/s/fq0QhojmcrnucJ7kDZPK1A

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34527

Windows Script Engine 内存损坏漏洞（CVE-2021-34448）：

脚本引擎中存在内存损坏漏洞，未授权的远程攻击者可通过诱导用户打开特制文件或访 问恶意网站进行利用，从而控制用户计算机系统，目前此漏洞已发现在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34448

Windows Kernel 远程代码执行漏洞（CVE-2021-34458）：

Windows 内核中存在远程代码执行漏洞，此漏洞影响 SR-IOV 虚拟机系统，CVSS 为 9.9 分官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34458

Exchange Server 远程代码执行漏洞（CVE-2021-34473）：

Microsoft Exchange Server 存在远程执行代码漏洞，未经身份验证的远程攻击者向服务器发送精心构造的请求，可在目标服务器上执行任意代码。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34473

Exchange Server 远程代码执行漏洞（CVE-2021-31206）：

此漏洞为 2021 Pwn2Own 竞赛上发现的 Exchange Server 漏洞之一，攻击者成功利用该漏洞可获取一定的服务器控制权限。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31206

Windows DNS Server 远程代码执行漏洞（CVE-2021-34494）：

Windows DNS 服务器存在远程执行代码漏洞，经过身份验证的攻击者通过向配置为 DNS

服务器发送特制的请求，可在目标主机上以 system 权限执行任意代码。官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34494

Windows Kernel 权限提升漏洞（CVE-2021-31979/CVE-2021-33771）：

Windows 存在两个内核权限提升漏洞，经过身份验证的本地攻击者可以运行特制的二进制文件，从而在目标主机上提升当前账户权限，目前已发现在野利用。

官方通告链接：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-31979
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-33771

## 三、影响范围

以下为重点关注漏洞的受影响产品版本，其他漏洞影响产品范围请参阅官方通告链接。

| 漏洞编号 | 受影响产品版本 |
| --- | --- |
| CVE-2021-34527 | 所有微软支持的 Windows 版本 |
| CVE-2021-34448 | Windows Server 2012 R2<br>Windows 10 Version 1607 for 32-bit Systems<br>Windows 10 for x64-based Systems<br>Windows 10 for 32-bit Systems<br>Windows 10 Version 20H2 for ARM64-based Systems<br>Windows 10 Version 20H2 for 32-bit Systems<br>Windows 10 Version 20H2 for x64-based Systems<br>Windows 10 Version 2004 for x64-based Systems<br>Windows 10 Version 2004 for ARM64-based Systems<br>Windows 10 Version 2004 for 32-bit Systems<br>Windows 10 Version 21H1 for 32-bit Systems<br>Windows 10 Version 21H1 for ARM64-based Systems<br>Windows 10 Version 21H1 for x64-based Systems<br>Windows 10 Version 1909 for ARM64-based Systems<br>Windows 10 Version 1909 for x64-based Systems<br>Windows 10 Version 1909 for 32-bit Systems<br>Windows Server 2019<br>Windows Server 2012<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1<br>Windows RT 8.1<br>Windows 8.1 for x64-based systems<br>Windows 8.1 for 32-bit systems<br>Windows 7 for x64-based Systems Service Pack 1<br>Windows 7 for 32-bit Systems Service Pack 1<br>Windows Server 2016<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems |

| 漏洞编号 | 受影响产品版本 |
| --- | --- |
| CVE-2021-34458 | Windows Server 2016 (Server Core installation)<br>Windows Server 2016<br>Windows Server, version 20H2 (Server Core Installation)<br>Windows Server, version 2004 (Server Core installation)<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2019 |
| CVE-2021-34473 | Microsoft Exchange Server 2019 Cumulative Update 9<br>Microsoft Exchange Server 2013 Cumulative Update 23<br>Microsoft Exchange Server 2019 Cumulative Update 8<br>Microsoft Exchange Server 2016 Cumulative Update 19<br>Microsoft Exchange Server 2016 Cumulative Update 20 |
| CVE-2021-31206 | Microsoft Exchange Server 2019 Cumulative Update 9<br>Microsoft Exchange Server 2019 Cumulative Update 10<br>Microsoft Exchange Server 2016 Cumulative Update 21<br>Microsoft Exchange Server 2016 Cumulative Update 20<br>Microsoft Exchange Server 2013 Cumulative Update 23 |
| CVE-2021-34494 | Windows Server, version 20H2 (Server Core Installation)<br>Windows Server, version 2004 (Server Core installation)<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2012 R2<br>Windows Server 2012 (Server Core installation)<br>Windows Server 2012<br>Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for x64-based Systems Service Pack 2<br>Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)<br>Windows Server 2008 for 32-bit Systems Service Pack 2<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)<br>Windows Server 2008 R2 for x64-based Systems Service Pack 1 |

| 漏洞编号 | 受影响产品版本 |
| --- | --- |
| CVE-2021-31979 | 所有微软支持的 Windows 版本 |
| CVE-2021-33771 | Windows Server, version 20H2 (Server Core Installation)<br>Windows Server, version 2004 (Server Core installation)<br>Windows Server 2019 (Server Core installation)<br>Windows Server 2019<br>Windows Server 2016 (Server Core installation)<br>Windows Server 2016<br>Windows Server 2012 R2 (Server Core installation)<br>Windows Server 2012 R2<br>Windows RT 8.1<br>Windows 8.1 for x64-based systems<br>Windows 8.1 for 32-bit systems<br>Windows 10 for x64-based Systems<br>Windows 10 for 32-bit Systems<br>Windows 10 Version 21H1 for x64-based Systems<br>Windows 10 Version 21H1 for ARM64-based Systems<br>Windows 10 Version 21H1 for 32-bit Systems<br>Windows 10 Version 20H2 for x64-based Systems<br>Windows 10 Version 20H2 for ARM64-based Systems<br>Windows 10 Version 20H2 for 32-bit Systems<br>Windows 10 Version 2004 for x64-based Systems<br>Windows 10 Version 2004 for ARM64-based Systems<br>Windows 10 Version 2004 for 32-bit Systems<br>Windows 10 Version 1909 for x64-based Systems<br>Windows 10 Version 1909 for ARM64-based Systems<br>Windows 10 Version 1909 for 32-bit Systems<br>Windows 10 Version 1809 for x64-based Systems<br>Windows 10 Version 1809 for ARM64-based Systems<br>Windows 10 Version 1809 for 32-bit Systems<br>Windows 10 Version 1607 for x64-based Systems<br>Windows 10 Version 1607 for 32-bit Systems |

## 四、漏洞防护

### 4.1 补丁更新

目前微软官方已针对受支持的产品版本发布了修复以上漏洞的安全补丁，强烈建议受影 响用户尽快安装补丁进行防护，官方下载链接：

https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Jul

注：由于网络问题、计算机环境问题等原因，Windows Update 的补丁更新可能出现失败。用户在安装补丁后，应及时检查补丁是否成功更新。

右键点击 Windows 图标，选择“设置(N)”，选择“更新和安全”-“Windows 更新”， 查看该页面上的提示信息，也可点击“查看更新历史记录”查看历史更新情况。

针对未成功安装的更新，可点击更新名称跳转到微软官方下载页面，建议用户点击该页 面上的链接，转到“Microsoft 更新目录”网站下载独立程序包并安装。

## 五、附录：漏洞列表

| 影响产品 | CVE 编号 | 漏洞标题 | 严重程度 |
|---|---|---|---|
| Windows | CVE-2021-33740 | Windows Media 远程代码执行漏洞 | Critical |
| Windows | CVE-2021-34494 | Windows DNS Server 远程代码执行漏洞 | Critical |
| Windows | CVE-2021-34497 | Windows MSHTML Platform 远程代码执行漏洞 | Critical |
| Windows | CVE-2021-34448 | Scripting Engine 内存泄露漏洞 | Critical |
| Windows | CVE-2021-34450 | Windows Hyper-V 远程代码执行漏洞 | Critical |
| Exchange Server | CVE-2021-34473 | Microsoft Exchange Server 远程代码执行漏洞 | Critical |
| Microsoft Dynamics | CVE-2021-34474 | Dynamics Business Central 远程代码执行漏洞 | Critical |
| Windows | CVE-2021-34439 | Microsoft Windows Media Foundation 远程代码执行漏洞 | Critical |
| Windows | CVE-2021-34503 | Microsoft Windows Media Foundation 远程代码执行漏洞 | Critical |

| 影响产品 | CVE 编号 | 漏洞标题 | 严重程度 |
| --- | --- | --- | --- |
| Windows | CVE-2021-34458 | Windows Kernel 远程代码执行漏洞 | Critical |
| System Center | CVE-2021-34464 | Microsoft Defender 远程代码执行漏洞 | Critical |
| System Center | CVE-2021-34522 | Microsoft Defender 远程代码执行漏洞 | Critical |
| Windows | CVE-2021-34527 | Windows Print Spooler 远程代码执行漏洞 | Critical |
| Windows | CVE-2021-31183 | Windows TCP/IP Driver 拒绝服务漏洞 | Important |
| Exchange Server | CVE-2021-31196 | Microsoft Exchange Server 远程代码执行漏洞 | Important |
| Exchange Server | CVE-2021-31206 | Microsoft Exchange Server 远程代码执行漏洞 | Important |
| Windows | CVE-2021-31947 | HEVC Video Extensions 远程代码执行漏洞 | Important |
| Windows | CVE-2021-31961 | Windows InstallService 权限提升漏洞 | Important |
| Power BI Report Server | CVE-2021-31984 | Power BI 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33743 | Windows Projected File System 权限提升漏洞 | Important |
| Windows | CVE-2021-33744 | Windows Secure Kernel Mode 安全功能绕过漏洞 | Important |
| Apps | CVE-2021-33753 | Microsoft Bing Search 欺骗漏洞 | Important |
| Windows | CVE-2021-33755 | Windows Hyper-V 拒绝服务漏洞 | Important |
| Windows | CVE-2021-33757 | Windows Security Account Manager Remote Protocol 安全功能绕过漏洞 | Important |
| Windows | CVE-2021-33758 | Windows Hyper-V 拒绝服务漏洞 | Important |
| Windows | CVE-2021-33759 | Windows Desktop Bridge 权限提升漏洞 | Important |
| Windows | CVE-2021-33760 | Media Foundation 信息披露漏洞 | Important |
| Windows | CVE-2021-33761 | Windows Remote Access Connection Manager 权限提升漏洞 | Important |
| Windows | CVE-2021-33763 | Windows Remote Access Connection Manager 信息披露漏洞 | Important |
| Windows | CVE-2021-33765 | Windows Installer 欺骗漏洞 | Important |
| Open Enclave SDK | CVE-2021-33767 | Open Enclave SDK 权限提升漏洞 | Important |
| Windows | CVE-2021-33771 | Windows Kernel 权限提升漏洞 | Important |

| 影响产品 | CVE 编号 | 漏洞标题 | 严重程度 |
| --- | --- | --- | --- |
| Windows | CVE-2021-33773 | Windows Remote Access Connection Manager 权限提升漏洞 | Important |
| Windows | CVE-2021-33774 | Windows Event Tracing 权限提升漏洞 | Important |
| Windows | CVE-2021-33780 | Windows DNS Server 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34441 | Microsoft Windows Media Foundation 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34442 | Windows DNS Server 拒绝服务漏洞 | Important |
| Windows | CVE-2021-34491 | Win32k 信息披露漏洞 | Important |
| Windows | CVE-2021-34492 | Windows Certificate 欺骗漏洞 | Important |
| Windows | CVE-2021-34493 | Windows Partition Management Driver 权限提升漏洞 | Important |
| Windows | CVE-2021-34444 | Windows DNS Server 拒绝服务漏洞 | Important |
| Windows | CVE-2021-34445 | Windows Remote Access Connection Manager 权限提升漏洞 | Important |
| Windows | CVE-2021-34446 | Windows HTML Platforms 安全功能绕过漏洞 | Important |
| Windows | CVE-2021-34496 | Windows GDI 信息披露漏洞 | Important |
| Windows | CVE-2021-34447 | Windows MSHTML Platform 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34498 | Windows GDI 权限提升漏洞 | Important |
| Windows | CVE-2021-34449 | Win32k 权限提升漏洞 | Important |
| Windows | CVE-2021-34499 | Windows DNS Server 拒绝服务漏洞 | Important |
| Windows | CVE-2021-34500 | Windows Kernel Memory 信息披露漏洞 | Important |
| Microsoft Office | CVE-2021-34501 | Microsoft Excel 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2021-34452 | Microsoft Word 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2021-34467 | Microsoft SharePoint Server 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2021-34518 | Microsoft Excel 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2021-34468 | Microsoft SharePoint Server 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2021-34469 | Microsoft Office 安全功能绕过漏洞 | Important |

| 影响产品 | CVE 编号 | 漏洞标题 | 严重程度 |
| --- | --- | --- | --- |
| Microsoft Office | CVE-2021-34520 | Microsoft SharePoint Server 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34521 | Raw Image Extension 远程代码执行漏洞 | Important |
| Exchange Server | CVE-2021-34523 | Microsoft Exchange Server 权限提升漏洞 | Important |
| Windows | CVE-2021-34476 | Bowser.sys 拒绝服务漏洞 | Important |
| Visual Studio Code | CVE-2021-34528 | Visual Studio Code 远程代码执行漏洞 | Important |
| Visual Studio Code | CVE-2021-34479 | Microsoft Visual Studio 欺骗漏洞 | Important |
| Windows | CVE-2021-31979 | Windows Kernel 权限提升漏洞 | Important |
| Windows | CVE-2021-33745 | Windows DNS Server 拒绝服务漏洞 | Important |
| Windows | CVE-2021-33746 | Windows DNS Server 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33749 | Windows DNS Snap-in 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33750 | Windows DNS Snap-in 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33751 | Storage Spaces Controller 权限提升漏洞 | Important |
| Windows | CVE-2021-33752 | Windows DNS Snap-in 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33754 | Windows DNS Server 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33756 | Windows DNS Snap-in 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33764 | Windows Key Distribution Center 信息披露漏洞 | Important |
| Exchange Server | CVE-2021-33766 | Microsoft Exchange 信息披露漏洞 | Important |
| Exchange Server | CVE-2021-33768 | Microsoft Exchange Server 权限提升漏洞 | Important |
| Windows | CVE-2021-33772 | Windows TCP/IP Driver 拒绝服务漏洞 | Important |
| Windows | CVE-2021-33775 | HEVC Video Extensions 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33776 | HEVC Video Extensions 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33777 | HEVC Video Extensions 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33778 | HEVC Video Extensions 远程代码执行漏洞 | Important |
| Windows | CVE-2021-33779 | Windows ADFS 安全功能绕过漏洞 | Important |

| 影响产品 | CVE 编号 | 漏洞标题 | 严重程度 |
| --- | --- | --- | --- |
| Windows | CVE-2021-33781 | Active Directory 安全功能绕过漏洞 | Important |
| Windows | CVE-2021-33782 | Windows Authenticode 欺骗漏洞 | Important |
| Windows | CVE-2021-33783 | Windows SMB 信息披露漏洞 | Important |
| Windows | CVE-2021-33784 | Windows Cloud Files Mini Filter Driver 权限提升漏洞 | Important |
| Windows | CVE-2021-33785 | Windows AF_UNIX Socket Provider 拒绝服务漏洞 | Important |
| Windows | CVE-2021-33786 | Windows LSA 安全功能绕过漏洞 | Important |
| Windows | CVE-2021-33788 | Windows LSA 拒绝服务漏洞 | Important |
| Windows | CVE-2021-34438 | Windows Font Driver Host 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34488 | Windows Console Driver 权限提升漏洞 | Important |
| Windows | CVE-2021-34489 | DirectWrite 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34440 | GDI+ 信息披露漏洞 | Important |
| Windows | CVE-2021-34490 | Windows TCP/IP Driver 拒绝服务漏洞 | Important |
| Microsoft Office | CVE-2021-34451 | Microsoft Office Online Server 欺骗漏洞 | Important |
| Windows | CVE-2021-34454 | Windows Remote Access Connection Manager 信息披露漏洞 | Important |
| Windows | CVE-2021-34504 | Windows Address Book 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34455 | Windows File History Service 权限提升漏洞 | Important |
| Windows | CVE-2021-34456 | Windows Remote Access Connection Manager 权限提升漏洞 | Important |
| Windows | CVE-2021-34457 | Windows Remote Access Connection Manager 信息披露漏洞 | Important |
| Windows | CVE-2021-34507 | Windows Remote Assistance 信息披露漏洞 | Important |
| Windows | CVE-2021-34508 | Windows Kernel 远程代码执行漏洞 | Important |
| Windows | CVE-2021-34459 | Windows AppContainer Elevation Of Privilege Vulnerability | Important |
| Windows | CVE-2021-34509 | Storage Spaces Controller 信息披露漏洞 | Important |
| Windows | CVE-2021-34460 | Storage Spaces Controller 权限提升漏洞 | Important |
| Windows | CVE-2021-34510 | Storage Spaces Controller 权限提升漏洞 | Important |

| 影响产品 | CVE 编号 | 漏洞标题 | 严重程度 |
| --- | --- | --- | --- |
| Windows | CVE-2021-34511 | Windows Installer 权限提升漏洞 | Important |
| Windows | CVE-2021-34461 | Windows Container Isolation FS Filter Driver 权限提升漏洞 | Important |
| Windows | CVE-2021-34512 | Storage Spaces Controller 权限提升漏洞 | Important |
| Windows | CVE-2021-34462 | Windows AppX Deployment Extensions 权限提升漏洞 | Important |
| Windows | CVE-2021-34513 | Storage Spaces Controller 权限提升漏洞 | Important |
| Windows | CVE-2021-34514 | Windows Kernel 权限提升漏洞 | Important |
| Windows | CVE-2021-34516 | Win32k 权限提升漏洞 | Important |
| Windows | CVE-2021-34466 | Windows Hello 安全功能绕过漏洞 | Important |
| Microsoft Office | CVE-2021-34517 | Microsoft SharePoint Server 欺骗漏洞 | Important |
| Exchange Server | CVE-2021-34470 | Microsoft Exchange Server 权限提升漏洞 | Important |
| Windows | CVE-2021-34525 | Windows DNS Server 远程代码执行漏洞 | Important |
| .NET Education Bundle SDK Install Tool,. NET Install Tool for Extension Authors | CVE-2021-34477 | Visual Studio Code .NET Runtime 权限提升漏洞 | Important |
| Visual Studio Code | CVE-2021-34529 | Visual Studio Code 远程代码执行漏洞 | Important |
| Microsoft Office | CVE-2021-34519 | Microsoft SharePoint Server 信息披露漏洞 | Moderate |

## 声明

NSFOCUS

# 安全态势

# 互联网安全威胁态势

## 行业动态回顾

### 1. Guess时尚品牌被勒索软件攻击，导致大量数据丢失

【概述】

攻击者破坏了Guess的1300名受害者的个人和银行数据。2月份针对时尚品牌Guess的勒索软件攻击与殖民管道攻击者DarkSide仍在造成破坏。Guess已经开始向1300名员工和承包商发信，这些人的个人和银行数据在这次入侵中被泄露。这封由BleepingComputer发布的信件为受害者提供了一年的免费信用监控和身份盗窃保护。但格斯向缅因州司法部长办公室提交的入侵通知文件称，在勒索软件攻击期间，超过1300人的信息被泄露，包括账号、借记卡和信用卡号码，甚至相关的安全代码、访问代码和个人识别号码。

【参考链接】

https://ti.nsfocus.com/security-news/4qYPQ

### 2. 攻击者窃取了大量的Humana客户的医疗数据

【概述】

专家发现了一个医疗数据库，其中包含属于美国保险巨头Humana客户的敏感健康保险数据，泄密事件发生在美国第三大健康保险公司，Humana通知其65,000名健康计划成员，该漏洞发生在2020年10月12日期间“分包商的员工向未经授权的个人泄露了医疗记录”。2020年12月16日，受数据泄露影响的一名患者向该公司提起诉讼。7月18日，我们联系了Humana以确认数据属于他们，但他们尚未做出回应。下载该数据库的一位论坛成员声称，该档案包含2020年的信息，而不是泄密者所建议的2019年的信息。如果论坛成员的说法属实，则泄露的数据库可能是2020年违规行为的一部分。话虽如此，泄密者发布的样本中发现的数据大多来自2019年，这可能表明它与之前的事件无关，可能是单独获取的。

【参考链接】

https://ti.nsfocus.com/security-news/4qYRM

### 3. “苦象”组织上半年针对我国的攻击活动分析

【概述】

近期，在梳理安全事件时，发现一批针对我国军工、贸易和能源等领域的网络攻击活动。攻击手法包括伪造身份向目标发送鱼叉邮件，投递恶意附件诱导受害者运行。经分析发现，这批活动具备APT组织“苦象”的历史特征，且在针对目标、恶意代码和网络资产等层面均存在关联，属于“苦象”组织在2021年上半年的典型攻击模式。

【参考链接】

https://ti.nsfocus.com/security-news/4qYOr

### 4. 黑客组织APT31利用办公路由器攻击法国组织

【概述】

法国国家网络安全局(ANSSI)下属的法国政府计算机应急准备小组CERT-FR警告说，与黑客组织APT31正通过在间谍活动中利用家庭和办公室路由器来攻击法国组织。

APT31，也称为Zirconium，以攻击政府、国际金融、航空航天和国防组织而闻名。该集团还攻击了高科技、建筑和工程、电信、媒体和保险公司。CERT-FR指出：“在执行侦察和攻击行动之前，威胁行为者使用受感染的路由器作为匿名中继。”CERT-FR没有回应信息安全媒体集团关于提供更多信息的请求，包括哪些组织受到了攻击。该组织提供了入侵IOC的指标，以帮助检测漏洞。“在日志中找到其中一个IOC，并不意味着整个系统已被攻陷，因此还需要进一步分析。

【参考链接】

https://ti.nsfocus.com/security-news/4qYRO

### 5. SolarWinds黑客利用iOS零日漏洞攻击iPhone

【概述】

SolarWinds 黑客利用位于浏览器引擎 WebKit 中的 iOS 零日漏洞以攻击更新的 iPhone，并通过瞄准全球手机赚取数百万美元。谷歌研究人员 Maddie Stone 和 Clement Lecitne 写道，攻击者很可能是俄罗斯政府资助的组织，利用当时未知的iOS 零日漏洞。怀疑黑客正在为俄罗斯外国情报局工作。

黑客通过LinkedIn向政府官员发送信息。微软研究人员透露，Nobelium 也向Windows 用户发送了恶意软件。

他们首先入侵了一个名为 Constant Contact 的在线营销公司的 USAID 帐户。然后，他们使用此帐户向属于美国民间对外援助和发展援助管理组织的地址发送电子邮件。

另一方面，攻击者的目标是 iOS 12.4 到 13.7 版本，甚至是更新的 iPhone。这些负载的任务是从各种网站收集身份验证 cookie，包括 Facebook、LinkedIn、谷歌和雅虎。数据后来通过WebSocket发送给黑客。

【参考链接】

https://ti.nsfocus.com/security-news/4qYS1

### 6. 攻击者利用AW工作流攻击Kubernetes集群

【概述】

Argo面向Web的仪表板的错误配置权限允许未经身份验证的攻击者在Kubernetes目标上运行代码，包括加密挖掘容器。安全研究人员警告说，Kubernetes集群正受到配置错误的ArgoWorkflows实例的攻击。

ArgoWorkflows是一个开源的容器原生工作流引擎，用于在Kubernetes上编排并行作业——以加快计算密集型作业的处理时间。它还通常用于简化容器部署。

与此同时，Kubernetes是一种流行的容器编排引擎，用于管理云部署。根据Intezer的一项分析，恶意软件运营商正在通过Argo将加密矿工放入云中，这要归功于某些实例可通过不需要外部用户身份验证的仪表板公开可用。因此，这些错误配置的权限可能允许威胁行为者在受害者的环境中运行未经授权的代码。

【参考链接】

https://ti.nsfocus.com/security-news/4qYRs

### 7. MosaicLoader恶意软件提供Facebook窃取程序和RAT

【概述】

一种名为MosaicLoader的Windows恶意软件正在全球范围内传播，充当全方位服务的恶意软件传送平台，被用来通过远程访问木马(RAT)、Facebookcookie窃取程序和其他威胁感染受害者。

根据Bitdefender研究人员的说法，他们发现加载程序通过搜索结果中的付费广告在全球范围内传播，目标是寻找盗版软件和游戏的人。它伪装成破解的软件安装程序，但实际上，它是一个下载程序，可以将任何有效负载传送到受感染的系统。

Bitdefender的研究人员解释说：“MosaicLoader背后的攻击者创建了一种恶意软件，可以在系统上传送任何有效载荷，使其作为传送服务有可能获利。”“它下载一个恶意软件喷射器，从命令和控制(C2)服务器获取URL列表，并从接收到的链接下载有效负载。”

研究人员观察到恶意软件喷射器提供Facebookcookie窃取程序，这些程序

会泄露登录数据——这允许网络攻击者接管帐户，创建传播恶意软件的帖子或导致声誉受损的帖子。

【参考链接】

https://ti.nsfocus.com/security-news/4qYRf

### 8. 攻击者窃取佛罗里达公寓倒塌受害者身份

【概述】

黑客正在窃取在公寓倒塌受害者中丢失人的身份。由于一群黑客以新的身份盗窃为目标，为佛罗里达州瑟夫赛德的尚普兰塔南公寓大楼部分倒塌而哀悼失去亲人的家庭现在被敦促检查他们已故亲属的信用方案。显然，网络犯罪分子正在观看新闻并窃取在广播期间阅读的受害者身份。Surfside市长CharlesBurkett告诉佛罗里达当地新闻台，执法部门正在努力追查网络犯罪分子。

【参考链接】

https://ti.nsfocus.com/security-news/4qYR1

### 9. 攻击者使用工程和网络钓鱼活动植入恶意软件攻击东京奥运会

【概述】

定于周五晚上开幕的东京奥运会已经成为威胁行为者的目标，然而，联邦调查局的网络部门发出警告，奥运会的电视广播很可能会受到威胁行为者的攻击。

联邦调查局的通知称：“攻击者可以在事件发生之前使用社交工程和网络钓鱼活动来获取访问权限或使用先前获得的访问权限来攻击恶意软件，以在事件期间破坏受影响的网络。”“社会工程和网络钓鱼活动继续为攻击者提供进行此类攻击所需的访问权限。”

联邦调查局补充说，奥运会将吸引那些想要“赚钱、散播混乱、增加恶名、诋毁对手和推进意识形态目标”的普通网络犯罪分子和民族国家行为者。

【参考链接】

https://ti.nsfocus.com/security-news/4qYRH

### 10. 攻击者攻击财富500强律师事务所

【概述】

美国律师事务所，以及众多大公司告知客户，入侵者可能已经窃取了他们的数据。今年2月份，该公司遭到勒索软件的攻击，现在正在遭受数据泄露影响。

这些客户涵盖众多行业，其中包括苹果、波音、英国航空公司、克莱斯勒、埃克森美孚、费雪-普莱斯、福特、本田、IBM、捷豹、孟山都、丰田和美国航空等公司。

周五，该公司在一份新闻稿中表示，它在2月27日意识到自己受到了勒索软件攻击。

【参考链接】

https://ti.nsfocus.com/security-news/4qYRe

### 11. 攻击者攻击沙特阿美的数据

【概述】

一名黑客声称从沙特阿拉伯石油和天然气巨头沙特阿美公司窃取了1TB的敏感数据。这家石油巨头的员工年收入超过2000亿美元，威胁行为者以500万美元的初始价格提供被盗数据。

BleepingComputer联系了该公司，该公司确认了第三方承包商的数据泄露，但指出该事件对Aramco的

运营没有影响。沙特阿美还告诉BleepingComputer，这不是勒索软件安全漏洞。

“沙特阿美最近意识到第三方承包商持有的有限数量的公司数据。”沙特阿美发言人告诉BleepingComputer。“我们确认数据的发布对我们的运营没有影响，公司继续保持稳健的网络安全态势。”ZeroX声称已在2020年利用零日漏洞从沙特阿美的基础设施中窃取数据。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYQY

### 12. 攻击者利用虚假的Flash更新攻击MacOs用户

**【概述】**

史蒂夫乔布斯称，攻击者借助虚假的Flash更新来攻击macOS用户，macOS使恶意行为者很难在Mac上安装恶意软件。但是自从Apple去年停止支持AdobeFlash以来，恶意软件作者就利用这一差距。欺骗用户下载和安装虚假的Flash安装程序。这些虚假安装程序可以容纳从广告软件到后门程序的任何内容，例如Shlayer和Bundlore。尽管这些安装程序通常没有数字签名并要求用户手动绕过Gatekeeper，但我们看到用户愿意绕过操作系统警告并手动安装这些安全风险。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYQQ

### 13. SonicWall的VPN硬件服务被攻击者严重攻击

**【概述】**

SonicWall发布了一个紧急安全警报，告知用户VPN设备正受到攻击。通知客户给企业安全VPN硬件打补丁，以防止安全漏洞勒索软件活动”。本次攻击的目标是该公司的安全移动接入(SMA) 100系列和安全远程接入(SRA)安全VPN设备的安全，包括未打补丁和寿命结束(EoL) 8.x固件。 在周四的一份安全公告中，该公司报告称，Mandiant的研究人员发现，“攻击者正在积极攻击”3款SMA 100型号和9款不再被SonicWall支持的老式sra系列安全VPN产品。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYQg

### 14. 黑客利用武器化的MS Office文档来攻击用户

【概述】

黑客利用武器化的MS Office文档或malspam活动中的其他社会工程策略来诱骗不知情的用户，让他们启用宏。 然而，事情发生了变化，研究人员发现的新攻击比以往任何时候都严重。根据McAfee实验室专家的一份报告，攻击者在这些活动中使用了一种新技术，即在目标计算机上执行宏代码之前，使用非恶意文件来禁用安全警告。

这意味着黑客下载恶意dll / ZLoader没有任何恶意代码在垃圾邮件附件宏。 因此，他们设计了一种新的策略来禁用宏安全警告。

【参考链接】

https://ti.nsfocus.com/security-news/4qYPm

### 15. KASEYA服务器被黑客攻击，发送垃圾邮件

【概述】

最近的Kaseya-VSA服务器漏洞攻击事件为网络犯罪分子提供了发布虚假Kaseya更新程序的机会。一些用户被欺骗下载在Kaseya上运行恶意软件的程序。据称，它来自Kaseya的“响应团队”，以及提供了一个工具的下载链接，该工具托管在合法的Kaseya.com 网站上，但单击该链接会将您带到不同的 URL。 因此Kaseya已经发表了一份声明，提醒他们的客户如果不确定链接的来源，不要点击任何链接。

【参考链接】

https://ti.nsfocus.com/security-news/4qYPp

### 16. 攻击者窃取了6亿LinkedIn的个人资料，并在网上出售这些资料

【概述】

在过去四个月里，LinkedIn似乎第三次经历了另一次由恶意行为者进行的大规模数据抓取。从数以亿计的LinkedIn用户资料中收集的数据又一次出现在一个黑客论坛上，目前正在以不公开的价格出售。这些信息虽然不是非常敏感，但仍可能被恶意行为者利用，LinkedIn拒绝将恶意抓取视为安全问题，这可能会让网络犯罪分子收集新的受害者数据而不受惩罚。 然而，这家社交媒体平台对此持不同看法。

【参考链接】

https://ti.nsfocus.com/security-news/4qYPE

### 17. WildPressure APT 组织利用Milum恶意软件攻击网站

【概述】

一直以中东的工业组织为目标的WildPressure APT 组织，现在被发现使用一种针对Windows和macOS的新恶意软件Milum。在2020年3月被发现的Milum恶意软件现已通过PyInstalle包进行了重组，其中包含了与Windows和macOS系统兼容的木马程序，被黑的网站可被该APT组织用来下载和上传文件并执行命令。

【参考链接】

https://ti.nsfocus.com/security-news/4qYPh

### 18. 攻击者攻击利用远程代码执行(RCE)漏洞ForgeRock访问管理平台

【概述】

攻击者利用ForgeRock访问管理平台上的一个预授权远程代码执行

(RCE)漏洞发起攻击。这些攻击是由ForgeRock的访问管理平台(Access Management)中的一个现已修补过的漏洞发起的，它用于前端web应用程序和远程访问设置。美国网络安全和基础设施安全局(CISA)警告称，该漏洞可能使攻击者能够在当前用户的环境下执行命令。

【参考链接】

https://ti.nsfocus.com/security-news/4qYPx

## 19. 网络攻击导致伊朗铁路网络“混乱”

【概述】

据国外媒体报道，由于网络攻击，伊朗的铁路服务和网络陷入“前所未有的混乱状态”，其全国的售票处疲于应付网络攻击，整体处于延误和取消状态。

IRIB报告称，用于在火车站向乘客显示到达和离开信息的电子板遭到破坏。董事会要求旅客拨打一个号码到达服务台以获取更多信息。然而，这个号码实际上已经被攻击者错误连接。

伊朗道路和城市发展部官员上周六证实了这次袭击。该部门表示：“在道路和城市发展部总部的工作人员计算机系统中断后，该部的技术专家正在调查这个问题。目前铁路服务网站已经恢复正常运作。”

【参考链接】

https://ti.nsfocus.com/security-news/4qYPl

## 20. Oracle Endeca服务器出现RCE漏洞

【概述】

Oracle Endeca Server是一个混合搜索分析数据库。它将来自不同的源系统组织成一个灵活的数据模型，从而减少了前期建模的需要。Oracle Endeca Server是为发现而设计的。通过其灵活的数据模型、柱状存储和内存分析，它将搜索、导航和分析统一起来，为结构化和非结构化数据提供快速的答案。

Oracle Endeca服务器存在命令执行漏洞。该漏洞是由于createDataStore方法的controlSoapBinding web服务导致，该服务包含一个允许注入任意命令的缺陷。

一个远程的、未经身份验证的攻击者可以通过向受影响的服务器发送一个特殊设计的请求来利用这个漏洞。 成功的利用可能导致任意命令执行的特权提高。

【参考链接】

https://ti.nsfocus.com/security-news/4qYPq

## 21. SonicWall SRA/SMA产品SQL注入漏洞

【概述】

2021年07月14日，漏洞编号为SNWLID-2021-0017，漏洞等级：严重，漏洞评分：9.8。Secure Remote Access (SRA)/Secure Mobile Access (SMA)产品均是SonicWall公司应用于企业管理安全接入的安全防护产品。该类产品的SQL注入漏洞将直接影响企业内部网络的安全性，具有极强的危害性。对此，建议广大用户及时将升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

【参考链接】

https://ti.nsfocus.com/security-news/4qYQc

## 22. 攻击者利用钓鱼邮件进行恶意软件攻击

【概述】

近期发现一个新的恶意电子邮件活动，该邮件声称包含Kaseya漏洞的补

丁，但实际上，它是恶意软件。这些钓鱼邮件包含了各种主题，围绕着“订单发货”，提示用户安装微软发布的补丁。

【参考链接】

https://ti.nsfocus.com/security-news/4qYP8

### 23. 黑客泄露了87000名GETTR用户的数据

【概述】

自2021年7月4日发布以来，支持特朗普的社交媒体平台GETTR已经遭受了两次攻击。

GETTR是一个受twitter启发的社交媒体平台。该网站于2021年7月4日上线，是美国前总统唐纳德·特朗普的前发言人杰森·米勒的创意。

一名黑客发布了一个数据库，声称其中包含了数千名GETTR用户的信息。Hackread.com已经包含了这些数据，可以确认，总计有87,973名用户的个人信息被在线曝光。

【参考链接】

https://ti.nsfocus.com/security-news/4qYP6

### 24. Nobelium黑客组织卷土重来，继续攻击微软新漏洞

【概述】

据微软公司表示，Nobelium黑客组织入侵了一名技术支持人员的电脑，并对其客户发动了暴力破解攻击。目前尚不清楚这名支持人员的电脑被入侵了多长时间，以及这次攻击是否殃及公司网络中由微软管理的机器。微软在周五下午晚些时候发表的一份简短声明中说，策划SolarWinds供应链攻击的黑客入侵了一名微软工作人员的电脑，并利用相应的权限对公司客户开展了针对性的攻击。

该黑客组织还利用密码喷洒和蛮力破解入侵了三家机构；简单来说，这次使用的技术通过用大量的登录猜测“轮番轰炸”登录服务器来获得对账户的未经授权的访问。微软表示，除了这三家未披露的机构外，密码喷洒攻击“都以失败而告终”。此后，微软已通知所有被攻击的目标，无论攻击是否成功。

【参考链接】

https://ti.nsfocus.com/security-news/4qYOS

### 25. googleplay中的恶意Android应用盗取Facebook凭据

【概述】

在googleplay上发现了9个盗取Facebook证书的恶意Android应用，在Google删除这些应用之前，这些应用总共安装了590万次。

恶意软件分析师称，这些应用程序功能齐全，因此受害者对他们将恶意软件下载到Android设备的事实一无所知。不过，它们会弹出窗口通知用户，要访问所有应用程序的功能并禁用应用程序内广告，用户需要登录他们的Facebook帐户。一旦他们这样做了，他们的密码和用户名就被获取了。

【参考链接】

https://ti.nsfocus.com/security-news/4qYOI

### 26. Kaseya：多达1500个组织遭受勒索软件攻击

【概述】

Kaseya在周一晚间发布的一份更新中表示，多达60名自己的客户受到了威胁。这些客户向其他客户提供IT管理服务，这些客户多达1500个。

攻击者使用的是由疑似俄罗斯Revil开发的勒索软件。Kaseya在另一份新闻稿中说，受影响的企业类型包括牙医办公室、小型会计师事务所和餐馆。

Revil组织声称已经入侵了100万个组织。该组织开始以7000万美元的比特币价格提供单一的通用解密工具，据说可以解密所有受害者的文件。但网络安全专家杰克·凯布尔当天晚些时候在twitter上表示，要价可能已经降至5000万美元，这表明受害者并没有集体急于支付。

【参考链接】

https://ti.nsfocus.com/security-news/4qYOD

### 27. 美国水务公司WSSC Water遭遇勒索软件攻击

【概述】

WSSC Water正在调查5月24日发生的一起勒索软件攻击事件，攻击目标是他们网络中运营非必要业务系统的一部分。

根据WJZ13 Baltimore的报道，该公司在几个小时后就删除了恶意软件，并锁定了威胁，然而，攻击者访问了内部文件。WSSC已经通知了联邦调查局、马里兰州总检察长以及州和地方国土安全官员。

该公司经营着过滤和污水处理厂，幸运的是，袭击没有影响水质，但调查仍在进行中。

【参考链接】

https://ti.nsfocus.com/security-news/4qYOs

### 28. 黑客诱骗微软签署了他们的恶意程序

【概述】

在最近的一篇报道中，微软已经承认他们签名了一个恶意驱动程序，现在它正在游戏环境中进行管理。经调查得知，该公司已签名的驱动程序为恶意Windows Rootkit，并持续针对游戏环境。

恶意软件分析师首先发现了恶意rootkit，他确认威胁行为者的目标是用户，特别是在东亚国家的一些用户。

微软公司已经注意到这次攻击，他们认为攻击者使用恶意驱动程序来欺骗他们的地理位置，以便欺骗系统并从任何地方玩游戏。

【参考链接】

https://ti.nsfocus.com/security-news/4qYOg

### 29. 逍遥法外的恶徒:一场在拉丁美洲的间谍活动

**【概述】**

ESET研究揭示了一个活跃的恶意活动，该活动使用新版本的旧恶意软件Bandook来监视其受害者。

2021年，我们检测到针对西班牙国家企业网络的持续活动，其中90%的检测发生在委内瑞拉。当将此活动中使用的恶意软件与之前记录的内容进行比较时，我们发现了此恶意软件（称为 Bandook）的新功能和更改。我们还发现，这场针对委内瑞拉的运动，自2015年以来一直很活跃，但不知何故一直没有记录。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYOR

### 30. 安全公司意外曝光Windows远程代码执行漏洞

**【概述】**

近日发布了一个针对关键Windows后台打印处理程序漏洞的概念验证漏洞，恶意用户可以利用该漏洞来破坏Active Directory域控制器。事情起因有些复杂，6月8日的，微软发布了针对CVE-2021-1675的修复程序，该漏洞被标记为提权漏洞。普通用户可以利用此漏洞以管理员身份在运行打印后台处理程序服务的系统上执行代码。然后在6月21日，没有任何解释，微软将该分类升级为更严重的远程代码执行漏洞。一组安全研究人员在看到该漏洞的严重性已升级后，决定发布针对打印假脱机服务中远程代码执行漏洞的概念验证漏洞，大概认为它现在已被修补。但是他们发布的漏洞利用代码针对的是一个与CVE-2021-1675类似但不完全相同的漏洞，结果这个漏洞被不法分子用来实施网络攻击。这个未修补的漏洞被称为PrintNightmare，可能需要微软单独更新才能完全解决它。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYOi

### 31. 西班牙电信巨头马斯莫维尔遭雷维尔勒索团伙袭击

**【概述】**

西班牙第四大电信运营商MasMovil成为了臭名昭著的Revil勒索软件团伙（又名Sodinokibi）的最新受害者。

从Hackread.com的网站上可以看到，这家勒索软件运营商在其官方博客上声称“下载了属于这家电信巨头的数据库和其他重要数据”。

作为黑客攻击的证据，该组织还分享了被盗的MasMovil数据的截图。

值得注意的是，在发表本文时，马斯莫维尔已经承认了勒索软件的攻击，但是，没有提及Revil团伙勒索赎金的要求。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYNK

### 32. 黑客入侵了美国大学医疗中心的数据服务器

**【概述】**

内华达州大学医疗中心医院暴露了一个安全漏洞，黑客入侵了其数据服务器，并在网上公布了被盗的个人信息的图片。

本周早些时候，黑客在其网站上公布了一些受害者的驾驶执照、护照和社会保障卡的图片。

拉斯维加斯评论杂志报道了这一消息，事件发生在6月中旬，执法部门正在调查这起袭击事件。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYNM

### 33. 领英史上最大规模数据泄露事件

**【概述】**

近日，研究人员发现有超过7亿领英用户数据在暗网出售，是领英史上最大规模的数据泄露事件。

6月22日，有黑客在暗网平台出售超过7亿的领英用户数据，并发布了一个包含100万领英用户的样本数据集。

研究人员查看该样本发现其中含有以下信息：

- 邮箱；
- 姓名；
- 电话号码；
- 家庭地址；
- 地理位置记录；
- 领英用户名和介绍的URL；
- 个人和职业经验、背景信息；
- 性别；
- 其他社交媒体账号和用户名。

这是领英史上最大规模的数据泄露事件。

卖家称完整的数据库中包含有7亿领英用户的个人信息。因为领英官方声称有7.56亿用户，也就是说有约92%的领英用户可以在该泄露的数据库中检索到个人的信息。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYNJ

### 34. Zyxel发出警告称其防火墙、VPN产品受到攻击

**【概述】**

台湾网络设备制造商Zyxel正在通知客户其部分企业防火墙和VPN产品正遭受一系列攻击，并建议用户在准备补丁时保持适当的远程访问安全策略。

该公司表示，攻击者的目标是其 USG、ATP、USG FLEX、ZyWALL 和 VPN 系列中启用了远程管理或 SSL VPN 的企业防火墙和 VPN 服务器。

该公司在一份声明中说："攻击者试图通过 WAN 访问设备，如果成功，他们将绕过身份验证，建立带有未知用户帐户的SSL VPN隧道，例如"zyxel_sllvpn"、"zyxel_ts"或"zyxel_vpn_test"，以此操纵设备的配置。"

据Zyxel报道，攻击者使用硬编码的帐户通过WANs访问设备。

【参考链接】

https://ti.nsfocus.com/security-news/4qYNw

### 35. Sodinokibi(REvil)勒索病毒最新变种，攻击Linux平台

【概述】

Sodinokibi(REvil)勒索病毒黑客组织此前一直以Windows平台为主要的攻击目标，目前首次发现这款勒索病毒在Linux平台上的最新变种样本，未来会不会有相关的安全事件爆发，需要持续关注。

【参考链接】

https://ti.nsfocus.com/security-news/4qYNp

### 36. 美国联邦调查局警告称，美国医疗保健网络遭到连续勒索软件攻击

【概述】

美国联邦调查局(FBI)已经确认至少16次针对美国医疗保健和急救网络的康迪勒索软件攻击。这些被攻击目标包括政府部门，如执法机构、急救人员和911系统。

根据联邦调查局发布的公告，一种广为人知的康迪勒索软件已经影响了美国的医疗保健系统和整个美国的医疗部门。这些袭击推迟或完全中断了医疗服务，使病人处于危险之中，并扰乱了依赖医院供应的当地社区。

【参考链接】

https://ti.nsfocus.com/security-news/4qYNl

### 37. 西部数据NAS设备网络攻击通告

【概述】

2021年06月28日，监测发现Western Digital发布了Recommended Security Measures for WD My Book Live and WD My Book Live Duo的通告。西部数据已经确定，该公司的 My Book Live 设备遭到了攻击者的入侵，这种入侵会导致设备被恢复出厂设置，数据也被全部擦除。My Book Live 设备在 2015 年进行了最后的固件更新，目前已不再享受官方的系统升级支持。

【参考链接】

https://ti.nsfocus.com/security-news/4qYNq

### 38. 美国梅赛德斯-奔驰称160万条记录曝光

【概述】

梅赛德斯-奔驰美国公司说，其一家供应商泄露了160万条与客户和感兴趣的买家有关的记录。大多数暴露的记录包含姓名、地址、电子邮件地址、电话号码以及可能购买车辆的信息。这些数据是在2014年1月1日至2017年6月19日之间在经销商和梅赛德斯-奔驰网站上收集的。

梅赛德斯-奔驰表示，将对那些驾驶执照号码、信用卡信息或社会保险号码被曝光的人提供为期两年的信用监控。该公司表示，它也在通知"适当的政府机构"。

【参考链接】

https://ti.nsfocus.com/security-news/4qYNj

### 39. Nobelium入侵了Microsoft客户服务帐户

【概述】

SolarWinds供应链攻击背后的同一个组织一直以微软的公司网络为目标，以获取特定组织的访问权。

在路透社获得一封发给客户的电子邮件后，微软正式宣布了这些攻击，该电子邮件解释说， Nobelium窃取了客户服务代理的凭据，以获取访问权限，并对微软客户发起攻击。微软在博客中说：“我们对使用的方法和战术的调查仍在继续，但我们看到了密码喷雾和暴力攻击。”

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYN4

### 40. 黑客摧毁了RSS新闻阅读器服务NewsBlur的数据库

**【概述】**

NewsBlur是一家总部位于美国的软件公司，运营着一项在线RSS新闻阅读器服务。在一名黑客清除了NewsBlur的数据库后，NewsBlur遭遇了服务中断。

据报道，当RSS阅读器过渡到Docker时，黑客(NewsBlur的创始人将其称为脚本小子)获得了对其数据库的访问权限。

这个过程绕过了一些防火墙规则，并将服务的MongoDB数据库暴露给公众。在过渡过程中，原来的主MongoDB集群被关闭，因此在攻击发生时它保持不变。

**【参考链接】**

https://ti.nsfocus.com/security-news/4qYN5

# 让安全更有效
# 绿盟科技安全服务
专业|灵活|高效

**咨询服务**
安全规划
合规咨询
信息安全管理体系咨询
应急体系建设
……

**可管理安全服务**
远程安全运维
全评估/测试服务
安全基线服务
应急响应
……

**安全评价**
外部检查辅导
安全指标体系度量
……

**安全研究**
渗透测试
源代码审计
业务安全测试
漏洞挖掘
……

**教育培训**
安全技能培训
安全意识教育
……


## THE EXPERT
## BEHIND GIANTS
## 巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

# 安全月报

绿盟科技金融事业部出品

**主办** / 绿盟科技金融事业部
**地址** / 北京市海淀区北洼路4号益泰大厦3层
**邮编** / 100089
**电话** / 010-59610688-1159
**传真** / 010-59610689
**网站** / www.nsfocus.com
**客户支持热线** / 400-818-6868
**股票代码** / 300369
**月报电子版下载** / https://www.nsfocus.com.cn/html/7/20/34/