In the Boxing Ring 2023年9月

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读2023年9月份的 In the **Boxing Ring**

本月，我们讨论梭子鱼 ESG 零日漏洞。 2023 年初，Barracuda Networks 发现其部分 ESG（电子邮件安全网关）设备出现异常流量。 随后，他们公开披露了标记为 CVE-2023-2868 的漏洞，这是一个远程命令注入漏洞，有被利用的证据。 然而，后来梭子鱼发布了一项更新，称所有受影响的设备都应该完全更换（而不仅仅是打补丁），无论固件或补丁级别如何，这震惊了安全行业。 这样的全球召回是史无前例的，表明问题比最初想象的要严重得多、根深蒂固得多。 在第 2 至第 3 页上，我们详细介绍了事件的时间线并更详细地讨论了该漏洞。

在第 4 页，我们重点介绍了本月的补丁星期二中将针对 Network Box 5 和我们的云服务发布的一系列增强功能和修复。

在其他新闻中，Network Box 很高兴地宣布与 Larix Industries 达成合作伙伴协议，为蒙古和哈萨克斯坦的客户提供我们的安全解决方案。 此外，Network Box 还参加了在蒙古国立大学举行的 SmartLife 技术论坛。 在本月的全球安全头条中，思科 VPN、瞻博网络防火墙和梭子鱼 ESG 设备都存在安全问题。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 2023

本月要闻:

BARRACUDA ESG 零日漏洞

2023 年 5 月中旬，Barracuda（网络安全设备制造商）发现其部分 ESG（电子邮件安全网关）设备出现异常流量。 这些设备可以过滤电子邮件中的病毒/垃圾邮件，并且可以部署为物理机或虚拟机。 Barracuda 随后于 2023 年 5 月 30 日公开披露了标记为 CVE-2023-2868 的漏洞，这是一个远程命令注入漏洞，有证据表明，至少在 2022 年 10 月就有人利用过该漏洞.

梭子鱼公司在其披露公告中透露，他们已于5月20日发布了补丁程序，这最初似乎更多的是类似的内容（只是另一个漏洞、另一个漏洞利用和解决该问题的补丁程序）。然而，6月6日，梭子鱼发布的更新震惊了安全行业，称所有受影响的设备都应彻底更换（而不仅仅是打补丁），无论固件或补丁级别如何。这样的全球召回是史无前例的，表明问题比最初想象的要严重得多，而且根深蒂固。

CVE-2023-2868

CVE 本身听起来相当恶意：

CVE-2023-2868

梭子鱼电子邮件安全网关（仅限物理设备形式）产品存在远程命令注入漏洞，影响版本 5.1.3.001-9.2.0.006。该漏洞源于未能全面消毒 .tar 文件（磁带归档文件）的处理。因此，远程攻击者可以特定的方式格式化这些文件名，从而通过 Perl 的 qx 操作员以电子邮件安全网关产品的权限远程执行系统命令。此问题已作为 BNSF-36456 修补程序的一部分得到修复。该修补程序已自动应用于所有客户设备。

Mandiant 为那些对更多技术方面感兴趣的人撰写了对该问题的全面分析：
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally
简而言之，当受影响的 Barracuda 设备收到一封包含附加“tar”的电子邮件时
(Unix/Linux Tape Archive) 文件，它尝试提取内容以进行进一步分析。 Barracuda 代码中的一个缺陷将未经清理的文件名列表作为参数传递给系统命令，从而使攻击者可以通过操纵存档中文件的文件名来控制实际执行的命令。

为什么如此严重?

利用此漏洞，攻击者可以完全控制受影响的设备。由于此类设备通常包含用于访问其他网络设备（例如 LDAP、FTP 和 SMB 服务器）的凭据，因此攻击者可以使用远程访问来利用连接网络上的其他计算机。 通过对Barracuda设备的完全访问，攻击者还可以安装后门、代理隧道和内核rootkit来完全破坏该设备。

考虑到妥协的程度，梭子鱼别无选择，只能建议完全更换受影响的设备。 他们根本无法确定一个简单的补丁是否可以消除所有漏洞的所有残留。

虽然在发行安全设备中包含这样一个根本性的弱点无疑是粗心的，但梭子鱼以开放和积极响应的方式处理后续工作值得称赞。

希望这次事件能够给网络安全界的每个人敲响警钟。 虽然我们已经习惯了漏洞-利用-补丁的循环，但我们必须意识到被利用的其他后果以及它们的严重程度。

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

在2023年9月5日星期二, Network Box 将会发布“星期二更新”, 包含部分改进和补丁。当地SOC将在接着的14天内部署该这些更新。

Network Box 5 新特性
2023年9月

本季度, Network Box 5 更新包括:

- 增强邮件扫描子系统的监控
- 邮件扫描大型 HTML 文档的性能改进
- Microsoft Outlook Office 脚本白名单（以避免可执行脚本策略阻止）
- 更新区域安全运营中心的 IP 范围
- 更新管理员和用户门户的 SSL 证书
- LDAP 搜索和多服务器故障转移的改进
- 引入从管理门户重新启动 IPSEC 服务的功能
- 允许设置管理门户网站和控制台的空闲超时
- SSL VPN 软件包的小幅升级

一般来说，以上更新不够影响正在进行的服务也不会需要重启，但是在一些情况下（根据配置），可能需要重启。如果需要以上安排的话，当地的SOC将会预先联系您。

如果您需要以上提及的更多相关信息, 请联系您当地的 SOC. 他们将安排部署和联系方式。

Network Box HIGHLIGHTS

SmartLife 2023年技术论坛

Network Box 参加了在蒙古国立大学举行的 SmartLife 技术论坛。 活动期间，Network Box 董事总经理 Michael Gazeley 向一众贵宾介绍了 Network Box 的托管网络安全服务。

全球安全头条

Bleeping Computer

Akira 勒索软件以思科 VPN 为目标，入侵组织机构
链接: https://bit.ly/45QG34F

The Hacker News

Juniper 防火墙、Openfire 和 Apache RocketMQ 受到新漏洞的攻击
链接: https://bit.ly/3L8rcu2

Bleeping Computer

FBI 警告称，已打补丁的梭子鱼 ESG 设备仍遭到黑客攻击
链接: https://bit.ly/3R5pIUU

Network Box 合作协议 Larix Industries Limited

Network Box 很高兴地宣布与 Larix Industries 达成合作伙伴协议，为蒙古和哈萨克斯坦的客户提供我们屡获殊荣的托管安全服务。

月刊主办

Mark Webb-Johnson
主编

Michael Gazeley
Kevin Hla
产品支持

Network Box HQ
Network Box USA
贡献者

订阅

Network Box CNNOC
cnnoc@network-box.cn

或者上门到:
深圳市福田区深南大道
竹子林求是大厦西座
920

+86 (755) 3336 1581
www.network-box.cn