伊顿安全公告

ETN-SB-2020-1008：Treck TCP/IP 堆栈中被称为“Ripple20”的多个安全漏洞

发布日期	受影响的伊顿产品	CVE ID	严重程度
2020 年 6 月 23 日 更新 2020 年 7 月 15 日 更新 2020 年 7 月 24 日 更新 2020 年 8 月 6 日 更新 2020 年 10 月 5 日 更新 2020 年 11 月 11 日 更新 2020 年 12 月 4 日	CL-7 电压调节控制器 Form 4D 自动开关控制器 Form 6 自动开关控制器 Edison Idea 和 IdeaPLUS 继电器（所有型号） Eaton G3/G3+ ePDU • 输入计量型 PDU • 计量输出型 PDU • 管理型 PDU • 高密度 HD PDU 网络管理卡迷你插槽 (NMC/Network-MS) 卡 • 带 Network-MS 卡的不间断电源 (UPS) • 带 Network-MS 卡的自动转换开关 (ATS16) Modbus-MS 卡 • 带 Modbus-MS 卡的不间断电源 (UPS)	多个 CVE	重要

概述

网络与基础设施安全局 (CISA) 发布了一份影响 Treck 公司 TCP/IP 堆栈的多个安全漏洞的相关报告，此堆栈在一些伊顿产品中用于实施 IPv4、IPv6、UDP、DNS、DHCP、TCP、ICMPv4 和 ARP。这些漏洞已经以“Ripple20”的名称统一发布。我们目前正在评估这些漏洞对我们产品的影响，并正在制定缓解方案来解决这些问题。

漏洞详细信息

报告的 Ripple20 漏洞的影响各不相同，包括对长度参数不一致性的不当处理、不正确的输入验证、双重释放、超范围读取、整数溢出或环绕、不正确的空终止和不正确的访问控制等类别。

有关更多详细信息，请参阅以下个别 CVE 的链接：

© 2020 伊顿，保留所有权利

伊顿安全公告

- CVE-2020-11896
- CVE-2020-11897
- CVE-2020-11898
- CVE-2020-11899
- CVE-2020-11900
- CVE-2020-11901
- CVE-2020-11902
- CVE-2020-11903
- CVE-2020-11904
- CVE-2020-11905
- CVE-2020-11906
- CVE-2020-11907
- CVE-2020-11908
- CVE-2020-11909
- CVE-2020-11910
- CVE-2020-11911
- CVE-2020-11912
- CVE-2020-11913
- CVE-2020-11914

受影响的伊顿产品和版本

以下伊顿产品直接或间接利用 Treck TCP/IP 堆栈，因此受到一个或多个报告漏洞的影响：

控制器和继电器产品 –

- CL-7 电压调节控制器 - 所有固件版本
- Form 4D 自动开关控制器 - 所有固件版本
- Form 6 自动开关控制器 - 固件版本 4.0 和更高版本
- Edison Idea 和 IdeaPLUS 继电器（所有型号）- 固件版本 4.0 和更高版本

配电和管理产品 –

- Eaton G3/G3+ ePDU – 所有固件版本
  - 计量输入 PDU
  - 计量输出 PDU
  - 托管 PDU
  - 高密度 PDU
- 网络管理卡迷你插槽 (NMC/Network-MS) 卡 – 所有固件版本
  - 带 Network-MS 卡的不间断电源 (UPS)
  - 带 Network-MS 卡的自动转换开关 (ATS16)
- Modbus-MS 卡 – 所有固件版本
  - 带 Modbus-MS 卡的不间断电源 (UPS)

注意 - 伊顿将在评估其他产品的同时继续更新此列表。

补救和缓解

补救

伊顿目前正在分析这些报告的漏洞对我们产品的影响，并准备采取适当的缓解方案。伊顿建议客户遵循网络安全最佳实践，进一步保护其设备，方法如下。有关补救和缓解的其他信息将在可用时发布。

© 2020 伊顿，保留所有权利

伊顿安全公告

- **Eaton G3/G3+ ePDU** – 新的固件版本 4.03.0000 已发布，用于修补安全问题。新版本可从此处下载 – http://powerquality.eaton.fr/support/software- drivers/downloads/epdu-firmware.asp?cx=80

- **CL-7 电压调节控制器** – 伊顿已修补受影响的产品固件并已发布新版本 1.15.2。最新版本可从此处下载 – https://my.eaton.com/

- **Form 4D** – 伊顿已修补受影响的产品固件并已发布新版本 1.9.0。最新版本可从此处下载 – https://my.eaton.com/

- **网络管理卡迷你插槽 (NMC/Network-MS) 卡** – 伊顿已修补受影响的产品固件并已发布新版本 LE。最新版本可从此处下载 - https://www.eaton.com/content/dam/eaton/products/backup-power-ups-surge-it-power- distribution/Firmware/connectivity/eaton-network-ms-firmware-le-download.zip

  或 UPS 网卡 | 监控 | 资源 | 伊顿 -> 导航至 Network-MS LE 版

- **Form 6 自动开关控制器** – 伊顿已修补受影响的产品固件并已发布新版本 5.5。最新版本可从此处下载 – https://my.eaton.com/

临时缓解措施

- 最大限度地减少所有控制系统设备和/或系统的网络暴露，并确保无法从互联网访问这些设备和/或系统。
- 找到防火墙后面的控制系统网络和远程设备，并将其与业务网络隔离。
- 当需要远程访问时，请使用安全方法（如虚拟专用网络 (VPN)），认识到 VPN 可能存在漏洞，应将 VPN 更新为最新可用版本。而且，认识到 VPN 的安全性仅与连接的设备一样。
- 使用采用 DNS-over-HTTPS 协议的内部 DNS 服务器进行解析。
- 其他缓解建议可在 ICS 报告 ICSA-20-168-01 和 CERT 协调中心漏洞说明 VU#257161 中找到。

一般安全最佳实践

- 限制所有控制系统设备和/或系统对外部网络的暴露，并确保无法从开放互联网直接访问这些设备和/或系统。
- 将控制系统网络和远程设备部署在隔离设备（例如，防火墙、数据单向控制器）之后，并将其与业务网络隔离。
- 对控制系统网络的远程访问应在严格的使用需求基础上提供。远程访问应使用安全方法，如虚拟专用网络 (VPN)，并更新为可用的最新版本。

© 2020 伊顿，保留所有权利

伊顿安全公告

- 在可行的情况下，定期将软件/应用程序更新/修补到可用的最新版本。
- 在所有设备和应用程序上启用审核日志。
- 禁用/停用联网设备上未使用的通信信道、TCP/UDP 端口和服务（例如，SNMP、FTP、BootP、DHCP 等）。
- 使用隔离设备（例如，防火墙、数据单向控制器）为具有共同安全要求的设备创建安全区域。
- 在首次启动后更改默认密码。使用复杂的安全密码或通行码。
- 定期对联网控制系统进行安全评估和风险分析。

如需详细了解网络安全最佳实践和利用伊顿的网络安全即服务，请参阅以下内容：

- 伊顿提供了一套网络安全评估和生命周期管理服务，以帮助识别漏洞并保护您的运营技术网络。这些服务可以帮助您完成建议的补救和缓解措施，并增强您的整体网络安全性。有关这些服务的更多信息，请访问 www.eaton.com/cybersecurityservices。 如果您需要立即支持，请致电 +1-800-498-2678 与服务代表联系。
- 配电系统的网络安全注意事项 (WP152002EN)
- 网络安全最佳实践检查清单提醒 (WP910003EN)

其他支持和信息

有关其他信息，包括关于我们产品的已报告漏洞列表以及如何处理这些漏洞，请访问我们的网络安全网站 www.eaton.com/cybersecurity，或通过 CybersecurityCOE@eaton.com 与我们联系。

法律免责声明：

在适用法律允许的最大范围内，本文档中提供的信息按“原样”提供，不提供任何形式的担保。伊顿、其附属公司、子公司和授权代表特此否认任何明示、暗示、法定或其他形式的担保和条件，包括但不限于任何对安全性、完整性、及时性、准确性、适销性或特定用途适用性的暗示担保和/或条件。某些司法管辖区不允许排除暗示担保或限制，因此上述限制可能不适用。在法律允许的范围内，伊顿或其附属公司、高级职员、董事和/或员工在任何情况下都不对任何形式的损失或损害负责，包括但不限于任何直接、间接、附带、特殊、法定、惩罚性、实际、已约定、惩戒性、后果性或其他损害，即使伊顿已被告知可能发生此类损害。使用本通知、本通知所含信息或与其相关的材料的风险由您自行承担。伊顿保留随时全权酌情更新或更改此通知的权利。

伊顿公司简介：

© 2020 伊顿，保留所有权利

伊顿安全公告

伊顿是一家动力管理公司。我们为客户提供高能效解决方案，以帮助客户更加高效、安全、可持续地有效管理电力、液压动力及机械动力。伊顿致力于通过运用动力管理技术和服务来改善生活品质和提升环境质量。伊顿拥有约 100,000 名员工，产品销往超过 175 个国家和地区。

© 2020 伊顿，保留所有权利

伊顿安全公告

版本控制：

日期	版本	注释
2020 年 6 月 23 日	v1.0	关于 Ripple20 的初步通知
2020 年 7 月 15 日	V1.1	更新了受影响产品的列表
2020 年 7 月 24 日	V1.2	更新了受影响的产品列表并更新了 ePDU 产品的缓解措施。
2020 年 8 月 6 日	V1.3	更新了 CL-7 产品的缓解措施。
2020 年 10 月 5 日	V1.4	更新了 Form 4D 的缓解措施
2020 年 11 月 11 日	V1.5	更新了网络管理卡迷你插槽 (NMC/Network-MS) 卡的缓解措施 • 带 Network-MS 卡的不间断电源 (UPS) • 带 Network-MS 卡的自动转换开关 (ATS16)
2020 年 12 月 4 日	V1.6	更新了 Form 6 的缓解措施

公司地址：

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com

© 2020 伊顿，保留所有权利