

施耐德电气安全通知

Easy UPS 在线监控软件

2023 年 12 月 12 日

概述

施耐德电气注意到在其 Easy UPS 在线监控软件产品中存在一个漏洞。

[Easy UPS 在线监控软件](#)是对 Easy UPS 进行配置和管理的软件。

如果不采取如下所述的缓解措施，就有提权的风险，从而导致以系统管理员权限删除任意文件。

受影响的产品和版本

产品	受影响的版本
Easy UPS 在线监控软件	2.6-GA-01-23116及之前的版本（Windows 10, 11, Windows Server 2016, 2019, 2022）

漏洞详细信息

CVE ID: CVE-2023-6407

CVSS v3.1 基本分数 5.3 | 中等 | CVSS:3.1/ AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H

CWE-22: 路径未限制在特定目录中（“路径遍历”）可能导致本地低权限攻击者在服务重启时进行任意文件删除。

关于漏洞详细信息的说明：漏洞的评分是使用 CVSS v3.1 中的基础分，未包括临时分和环境分。施耐德电气建议客户基于最终用户的特定组织情况评判 CVSS 环境分，并在评判时考虑部署环境中的缓解措施。环境分可以基于客户的具体环境对本文档所述漏洞的严重程度做出更精细的评判。

补救

施耐德电气安全通知

受影响的产品	补救措施
Easy UPS 在线监控软件 Windows 10, 11, Windows Server 2016、 2019 和 2022 v2.6-GA-01- 23116 及之前的版本	<p>Easy UPS 在线监控软件 v2.6-GA-01-23248 提供漏洞的修复，该软件可运行在受微软支持的 Windows 10, 11, Windows Server 2016、2019 和 2022 上。您可以通过这个链接下载：https://www.apc.com/us/en/faqs/FAQ000260058/。</p> <p>Easy UPS 在线监控软件已经与它所管理的 Easy UPS 在线 SNMP 卡 (APV9601, APVS9601) 同时停止支持。</p> <p>注意：本补丁适用于各种类别的 Easy UPS 在线监控软件。</p> <p>施耐德电气建议仍在使用的 Easy UPS 在线监控软件管理 Easy UPS Online (SRV/SRVS) 的客户改用 PowerChute 关机软件串口版来通过串口/USB 关闭或监控设备或改用 PowerChute 网络关机软件来通过网络关闭或监控设备。您可以通过以下链接获取 PowerChute 软件的更多信息： https://www.apc.com/pcss https://www.apc.com/pcns</p>

客户应该采取合适的方式给他们的系统安装补丁。我们强烈建议客户采取备份机制并在一个开发测试环境或离线基础设施中评估补丁的影响。如果您需要卸载补丁的协助，请联系施耐德电气的[客户关爱中心](#)。

为确保您获悉所有更新，包括有关受影响产品和修复计划的详细信息，请在此处订阅施耐德电气的安全通知服务：

<https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp>

如果客户选择不采取上述补救措施，他们应当立即采取以下一般信息安全建议以降低漏洞被利用的风险：

施耐德电气安全通知

一般信息安全建议

我们强烈推荐以下行业信息安全最佳实践。

- 将控制和功能安全系统网络和远程设备置于防火墙后面，并将它们与办公网络隔离。
- 安装物理控制措施，使未经授权的人员无法接触到您的工业控制和功能安全系统、组件、外围设备和网络。
- 将所有控制器锁在柜子中，切勿让它们处于编程模式。
- 切勿将编程软件连接到除用于该设备的网络之外的任何网络。
- 在终端或连接到这些网络的任何节点中使用之前，扫描与隔离网络（如 CD、USB 驱动器等）进行移动数据交换的所有方法。
- 未经适当的净化措施之前切勿允许连接过除预期网络外的任何其他网络的移动设备连接到安全或控制网络。
- 最大限度地减少所有控制系统设备和系统在网络中的暴露，确保它们无法从 Internet 访问。
- 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，应更新至最新可用版本。此外，要明白 VPN 仅能做到和连接的设备一样安全。

有关更多信息，请参阅施耐德电气建议的[信息安全最佳实践文档](#)。

鸣谢

施耐德电气认可以下研究人员识别并帮助协调对此漏洞的响应：

CVE	研究人员
CVE-2023-6407	Trend Micro Zero Day Initiative Tenable Network Security

了解更多信息

本文档概述了已识别的漏洞和所需采取的相应的缓解措施。有关更多如何保护您设备的详细信息和帮助，请联系您当地的施耐德电气代表或施耐德电气工业信息安全服务：

<https://www.schneider-electric.cn/zh/work/services/cybersecurity-services/>。这些组织将充分了解这一情况，并可在整个过程中为您提供支持。

有关施耐德电气产品信息安全的更多信息，请访问公司的网络安全支持门户：

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

施耐德电气安全通知

法律免责声明

本通知文档、此处包含的信息以及与其关联的任何材料（统称为“通知”）旨在帮助概述已识别的情况和建议的缓解措施、补救、修复和/或一般安全建议，并按“原样”提供而不提供任何形式的担保或保证。施耐德电气不提供与本通知相关的所有明示或暗示担保，包括对适销性或特定用途适用性的担保。施耐德电气不保证该通知将解决已识别的情况。在任何情况下，施耐德电气都不对与本通知相关的任何损害或损失负责，包括直接的、间接的、附带的、后果性的、业务利润损失或特别损害，即使施耐德电气已被告知这种损害的可能性。您使用此通知的风险由您自己承担，您对因使用此通知而可能对系统或资产造成的任何损害或其他损失全权负责。施耐德电气保留随时自行更新或更改此通知的权利。

关于施耐德电气

施耐德电气的目标是赋能所有人对能源和资源的最大化利用，并确保每一个人，在任何时间，在任何地点都能尽享 Life Is On。

我们提供能源和自动化数字解决方案，以实现高效和可持续。我们将世界领先的能源技术、自动化技术、软件及服务融合于整体解决方案之中，服务于家居、楼宇、数据中心、基础设施和工业市场。

我们致力于释放开放的、全球性的、创新的社区的无限可能性，并对我们有意义、包容和赋能的价值观充满热情。

www.se.com

版本控制：

1. 0. 0版 2023年12月12日	首次发布
-------------------------	------