Microsoft Security Vulnerability: Disable Print Spooler Service

Date: July 13, 2021

Microsoft has released a critical vulnerability for Print Spooler Service in multiple versions of Microsoft Windows. At GE, cybersecurity is a top priority and we actively monitor security vulnerabilities. Microsoft has thus far released a mitigation strategy to reduce the risk of this vulnerability. Please see below to disable the Print Spooler Service from Microsoft.

For On-Site Monitors (OSMs) connected to the M&D Network, the steps below have already been taken to remotely disable the Print Spooler Service, as well as applying the security patches Microsoft has already released for all supported versions of Windows.

Workarounds and Mitigation

Applicable Equipment: See the below CVE's for applicable Microsoft OS Versions

CVE-2021-34527- A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations.

To exploit the vulnerability, an attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

At this time, it has been found that the Microsoft released patches may not fix the vulnerability. GE recommends disabling the print spooler service for the time being until there is a fix. Once a patch has been released and validated to mitigate the risk, we will publish another advisory with an update.

HTTPS://MSRC.MICROSOFT.COM/UPDATE-GUIDE/EN-US/VULNERABILITY/CVE-2021-34527

Disable Print Spooler Service

GE recommends that the Print Spooler Service is disabled. Disabling this service mitigates the risk of this vulnerability. There are three options in the article below to disable, GE recommends disabling by Group Policy.

Please see the following article and disable the service by Group Policy-
https://www.pdq.com/blog/printnightmare-new-zero-day-exploit-using-the-windows-print-spooler/

Please note that there is no patch released or validated yet that fixes the vulnerability. Therefore, we are solely recommending to disable Print Spooler Service at this time.

GE always recommends users take defensive measures to minimize the risk of exploitation of vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Additional Information

Microsoft patch portal:

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

Helpful Articles:

https://www.pdq.com/blog/printnightmare-new-zero-day-exploit-using-the-windows-print-spooler/

Tenable article:

https://www.tenable.com/blog/cve-2021-34527-microsoft-releases-out-of-band-patch-for-printnightmare-vulnerability-in-windows

CISA portal:

https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.