Remote Desktop Services Remote Code Execution Vulnerability

Date: June 1, 2019

Summary:

A security vulnerability has been identified by Microsoft that impacts the Windows Operating System (OS). HMIs using the Windows 7 OS should be patched using the update available from Microsoft. The vulnerability may allow a remote attacker to gain full unauthorized access to the control system Human Machine Interface (HMI).

Affected Products:

- Windows 7 HMI
- Dell-Wyse 7020 Windows 7 Embedded Quad Video RDP Thin Client

Detailed Description:

A remote code execution vulnerability exists in the Windows 7 OS, that if exploited, could result in an unauthenticated attacker having the ability to install programs, change or delete files or create user accounts with full system access. Details of the vulnerability and other affected operating systems are available on the Microsoft Website:

https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remotedesktop-services-cve-2019-0708/

GE HMIs using Windows 7 with Remote Desktop Protocol Services enabled are impacted by this vulnerability. For reference, the following Microsoft operating systems are impacted:

- Microsoft Windows Server 2008 R2 for x64-based Systems SP1
- Microsoft Windows Server 2
- 008 R2 for Itanium-based Systems SP1
- Microsoft Windows Server 2008 for x64-based Systems SP2
- Microsoft Windows Server 2008 for Itanium-based Systems SP2
- Microsoft Windows Server 2008 for 32-bit Systems SP2
- Microsoft Windows 7 for x64-based Systems SP1
- Microsoft Windows 7 for 32-bit Systems SP1
- Microsoft Windows Server 2003 SP2 x86
- Microsoft Windows Server 2003 x64 Edition SP2
- Microsoft Windows XP SP3 x86
- Microsoft Windows XP Professional x64 Edition SP2
- Microsoft Windows XP Embedded SP3 x86

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL

Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Recommendations:

GE recommends HMIs and any other customer installed windows computers be updated with the Microsoft patch as soon as possible. Patches may be downloaded from Microsoft: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Note: GE has verified the patch only for the GE build of the HMI using Windows 7. No other operating systems have been validated. GE also recommends the Dell-Wyse RDP thin clients be updated according to the manufacturer's instructions: https://www.dell.com/support/article/us/en/04/sln317327/dsa-2019-085-dell-thin-client-securityupdate-for-microsoft-remote-desktop-services-remote-code-execution-vulnerability?lang=en

Workarounds and Precautions:

Until the appropriate patch is applied, using the corresponding Microsoft documentation, the following precautions may be performed immediately to limit the exposure to exploitation:

- Disable RDP services where not needed
- Enable Network Level Authentication (NLA)
- Limit or block port 3389 access to the control system where feasible

To minimize the risk of exposure to this and any other vulnerabilities, GE recommends a defense in depth approach to protecting critical process control equipment. Guidance on technology and best practices to secure GE controllers from Cyber-attack can be found in the published Mark VIe Control Systems Secure Deployment Guide (GEH-6839). https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0026895

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.