Life Is On Schneider Electric

Schneider Electric Security Notification

CVE-2019-0708 Microsoft Remote Desktop Services (BlueKeep) (V1.4)

12 July 2019 (12 November 2019)

Overview

Update: Schneider Electric is aware of an exploit available that targets the BlueKeep vulnerability. Our customers should urgently consider applying the remediations detailed in this document.

Schneider Electric is actively investigating the impact of the Microsoft Remote Desktop Services (BlueKeep) vulnerability on our offers. Offer specific information will be posted here as it becomes available.

Schneider Electric offers with special or specific recommendations applicable to this vulnerability are listed below. As a general recommendation from Schneider Electric, we advise customers to refer immediately to Microsoft's Security Update Guide for further information and guidance for any affected systems that may or may not serve as a runtime environment for Schneider Electric software and services. Microsoft warns that this vulnerability is wormable and all affected systems should be updated as soon as possible.

Customers should proceed with caution when applying these patches to critical operating systems and/or performance-constrained systems. We strongly recommend evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure.

Downloads for in-support versions of Windows can be found in the Microsoft Security Update Guide. Customers who use an in-support version of Windows and have automatic updates enabled are protected once the patches are applied. Microsoft recommends that Windows 2003 and Windows XP users should further consider upgrading to the latest version of Windows to protect themselves from this vulnerability. Fixes have been made available by Microsoft for these out-of-support versions of Windows in KB4500705.

Schneider Electric continues to monitor and track vendor research into this vulnerability.

Please refer to this link for more Information on the Microsoft RDS Vulnerability:
https://www.schneider-electric.com/en/download/document/SESB-2019-136-02/

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2019-0708**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability.

Affected Products and Remediation

Affected Product	Remediation
HMIG5U, PFXSP5B40 (Windows Embedded Standard 7 SP1 32bit) ***All versions***	*This product is End of Life* Apply Security Patch provided by Microsoft for existing install base at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
HMIG5U2, PFXSP5B41 (Windows Embedded Standard 7 SP1 32bit) ***All versions***	*Fixed versions planned for December 2019* Apply Security Patch provided by Microsoft for existing install base at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
All versions - HMIBMU, HMIBMP (Windows 7 Ultimate SP1 64bit) - PS5000 Series (Windows 7 Ultimate SP1 64bit) - HMIBMU, HMIBMP (Windows Embedded Standard 7 SP1 64bit) - PS5000 Series (Windows Embedded Standard 7 SP1 32bit/64bit)	*Fixed versions planned for after February 2020* Apply Security Patch provided by Microsoft for existing install base at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- HMIBSO (Windows Embedded Standard 2009 32bit) - PE4000B Series (Windows Embedded Standard 2009 32bit)	*This product will be End of Life as of July 2019* Apply Security Patch provided by Microsoft for existing install base at https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

All versions - HMIPU, HMIPP (Windows7 Ultimate SP1 64bit) - PS4600 Series (Windows7 Ultimate SP1 64bit) - HMIPU, HMIPP (Windows Embedded Standard 2009 32bit) - PS4600 Series (Windows Embedded Standard 2009 32bit) - HMIPU, HMIPP (Windows Embedded Standard 7 SP1 32bit) - PS4600 Series (Windows Embedded Standard 7 SP1 32bit) - HMIBSU (Windows Embedded Standard 7 SP1 32bit) - PE4000B Series (Windows Embedded Standard 7 SP1 32bit)	*This product will be End of Life as of July 2019* Apply Security Patch provided by Microsoft for existing install base at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
All versions - HMIG5UL8A (Windows Embedded Standard 7 SP1 32bit) - PFXSP5B41S8A (Windows Embedded Standard 7 SP1 32bit)	*This product will be End of Life as of December 2019* Apply Security Patch provided by Microsoft for existing install base at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
All versions - HMIG5UL8B (Windows Embedded Standard 7 SP1 32bit) - PFXSP5B41S8B (Windows Embedded Standard 7 SP1 32bit)	*Fixed planned in versions manufactured after August 2019* Apply Security Patch provided by Microsoft for existing install base at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
All versions - HMIRSPSXR6S01 (Windows Server 2008 Standard R2) - HMIRSP (Windows7 64bit) - HMIRXOHCA3W01 (Windows7 32bit) - HMIRSOHPA3W01 (Windows7 64bit) - HMIRXOHCA3001 (Windows7 Ultimate 64bit) - HMIRSUH3A3701 (Windows7 Ultimate 64bit) - HMIRSUS3A3701 (Windows7 Ultimate 64bit)	*Fixed versions planned after February 2020* Apply Security Patch provided by Microsoft for existing install base at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

TelevisGo ***All versions prior to July 2019***	*Fixed in all BoxPC manufactured after July 15 2019* The vulnerability impacts the Windows 7 Operating system of the BoxPC hosting the TelevisGo application. The hot fix https://www.eliwell.com/it/search.html?q=TelevisGo included in all BoxPC manufactured after July 15, 2019, will be distributed to apply the patches to the BoxPCs already in the field We also strongly recommend to install Windows Security Update KB4499175 as a complementary remediation : https://support.microsoft.com/en-us/help/4499175/windows-7-update-kb4499175
EcoStruxure Foxboro DCS EcoStruxure Foxboro SCADA ***All versions prior to May 2019***	*Fixed in all versions running: Windows 7 and Server 2008 and Windows XP and Server 2003* Schneider Electric has evaluated the Microsoft Security patches for this vulnerability and made them available to customers through Global customer Support Website https://pasupport.schneider-electric.com/home.asp We recommend that customers install the Security patches following the instructions in https://pasupport.schneider-electric.com/km/index?page=content&id=ADV307&cat=SECURITY_ISSUE&actp=LIST
ADMS ***Versions 3.2, 3.3***	Microsoft KB4499180 and KB4500331 https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
ADMS ***Versions 3.4, 3.5, 3.6***	Microsoft KB4499164 Monthly rollup https://support.microsoft.com/en-us/help/4499164/windows-7-update-kb4499164
Conext Control - Server ***Windows Server 2008 R2 SP1***	Apply the following Microsoft security patch to the Conext Control server if it is running Windows Server 2008 R2 SP1: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

General Security Recommendations

Schneider Electric Security Notification

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- 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.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

Schneider Electric Security Notification

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *12 July 2019*	Original Release
Version 1.1 *10 September 2019*	Exploit information added to Overview Section (page 1)
Version 1.2 *11 September 2019*	Product versions updated (page 6)
Version 1.3 *24 September 2019*	Added “Conext Control” to list of affected products (page 6)
Version 1.4 *12 November 2019*	Updated “Conext Control” affected products and remediation detail (page 6)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.10.24 11:07:41 -04'00'