Schneider Electric Security Notification

Microsoft Remote Desktop Services - DejaBlue (V5.0)

24 September 2019 (12 October 2021)

Overview

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

Schneider Electric is aware of seven Remote Desktop Services (RDS) vulnerabilities disclosed on 13 August 2019 affecting a wide range of Microsoft operating systems including Windows 7 SP1, Windows Server 2008 R2 SP1, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, and all supported versions of Windows 10, including server versions.

Four of these vulnerabilities are remote-code execution vulnerabilities which, if exploited, could enable an attacker to execute arbitrary code on the target system, thereby allowing the attack to install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft warns that, similar to the previously disclosed BlueKeep vulnerability that affected older Windows operating systems, two of these new remote-code execution vulnerabilities (dubbed named DejaBlue by security researchers) are 'wormable,' meaning the malware can propagate from vulnerable system to vulnerable system without any user interaction.

Schneider Electric continues to assess how the newly disclosed RDS vulnerabilities impact our offers. In the meantime, we advise customers to refer immediately to both Microsoft's security updates webpage for further information and guidance for any affected systems that may or may not serve as a runtime environment for Schneider Electric offers as well as the Affected Products and Remediation section of this document below. As a recommended mitigation by Microsoft, customers can also consider disabling Remote Desktop Services if they are not required.

Please refer to this link for more Information on the Microsoft RDS (DejaBlue) Vulnerability:

https://www.schneider-electric.com/en/download/document/SESB-2019-228-01/

October 2021 Update: Added remediations for *Conext™ Advisor 2 Cloud, Conext™ Advisor 2 Gateway, Conext™ Control V2 Gateway* (page 3).

Vulnerability Details

CVE ID: **CVE-2019-1181**

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'. This CVE ID is unique from CVE-2019-1182, CVE-2019-1222, CVE-2019-1226.

CVE ID: **CVE-2019-1182**

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'. This CVE ID is unique from CVE-2019-1181, CVE-2019-1222, CVE-2019-1226.

CVE ID: **CVE-2019-1222**

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'. This CVE ID is unique from CVE-2019-1181, CVE-2019-1182, CVE-2019-1226.

CVE ID: **CVE-2019-1226**

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 Service Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1181, CVE-2019-1182, CVE-2019-1222.

CVE ID: **CVE-2019-1224**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

An information disclosure vulnerability exists when the Windows RDP server improperly discloses the contents of its memory, aka 'Remote Desktop Protocol Server Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1225.

CVE ID: **CVE-2019-1225**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

An information disclosure vulnerability exists when the Windows RDP server improperly discloses the contents of its memory, aka 'Remote Desktop Protocol Server Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1224.

CVE ID: **CVE-2019-1223**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.

Affected Products and Remediation

Affected Product	Remediation
Conext™ Advisor 2 Cloud **V2.02 and prior**	Microsoft Windows 10 includes a fix for this vulnerability and is available for download here: https://www.microsoft.com/en-in/software-download/windows10 *Reboot is required*
Conext™ Advisor 2 Gateway **V1.28.45 and prior**	Microsoft Windows 10 includes a fix for this vulnerability and is available for download here: https://www.microsoft.com/en-in/software-download/windows10 *Reboot is required*
Conext™ Control V2 Gateway **V2.6 and prior**	Microsoft Windows 10 includes a fix for this vulnerability and is available for download here: https://www.microsoft.com/en-in/software-download/windows10 *Reboot is required*

Schneider Electric Security Notification

EcoStruxure ADMS v3.3, v3.4	*Apply the following security patch.* Microsoft KB4512506 https://support.microsoft.com/en-us/help/4512506/windows-7-update-kb4512506
EcoStruxure ADMS V3.5, v3.6	*Apply the following security patches.* Microsoft KB4512506 and KB4512488 https://support.microsoft.com/en-us/help/4512506/windows-7-update-kb4512506 https://support.microsoft.com/en-us/help/4512488/windows-8-1-update-kb4512488
EcoStruxure ADMS V3.7, and AGMS software	*Apply the following security patch.* Microsoft KB4512517 https://support.microsoft.com/en-us/help/4512517/windows-10-update-kb4512517
EcoStruxure ADMS V3.8	*Apply the following security patch.* Microsoft KB4512517 and KB4511553 https://support.microsoft.com/en-us/help/4512517/windows-10-update-kb4512517 https://support.microsoft.com/en-us/help/4511553/windows-10-update-kb4511553
EcoStruxure Substation Operation Gateway (formerly known as PACiS Gateway)	Affected by: CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, CVE-2019-1223, CVE-2019-1224, CVE-2019-1225, CVE-2019-1226 Upgrade to version 3.606.100.600.1 or newer.

EcoStruxure Substation Operation User Interface (formerly known as PACiS SUI)	Affected by: CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, CVE-2019-1223, CVE-2019-1224, CVE-2019-1225, CVE-2019-1226 *Schneider Electric is currently validating the Microsoft patches as part of an upcoming product update. We advise customers not to enable Remote Desktop Services (RDS), or as a mitigation, to prevent access to this service from unauthorized sources.*
Schneider Electric Exchange (https://exchange.se.com) **Digital Offers EcoStruxure Technology Platform (ETP)**	Host platforms have been patched.
Multiple Operating System versions are affected for the following products. Refer to the appendix for detailed OS list. - **HMIBMU, HMIBMP** - **PS-5000 Modular Type (Core i7/Celeron Model)** - **PS-5000 Modular Type (Core i7/Celeron Model)** - **HMIPEP** - **PS-5821W** - **HMIPSP** - **PS-5711W, PS-5811W** - **HMIPSO** - **PS-5501W, PS-5701W** - **HMIPP** - **PS-4600 (Core i3)** - **HMIPU** - **PS-4600 (Celeron)** - **HMIBSU** - **PE-4000B (N2600)** - **HMIRSP** - **HMIRXO** - **HMIRSO** - **HMIRSU** - **HMIBP** - **PS-4000B (P8400)** - **HMIBU** - **PS-4000B (N270)** - **PS-4700, PS-4800 (P8400)** - **PS-4700, PS-4800 (N270)**	Affected by: CVE-2019-1181, CVE-2019-1182 *The vulnerable service, Remote Desktop Services (RDS), is disabled by default on these products. Schneider Electric is currently validating the Microsoft patches.* *We advise customers not to enable RDS, or as a mitigation, to prevent access to this service from unauthorized sources.*

- **HMIBMO, HMIBMI** on Windows 10 IoT Enterprise LTSB 2016 64bit - **PS-5000 Modular Type (Atom Model)** on Windows 10 IoT Enterprise LTSB 2016 64bit - **HMIBMU, HMIBMP** on Windows 10 IoT Enterprise LTSB 2016 64bit - **PS-5000 Modular Type (Core i7/Celeron Model)** on Windows 10 IoT Enterprise LTSB 2016 64bit - **HMIPEP** on Windows 10 IoT Enterprise LTSB 2016 64bit - **PS-5821W** on Windows 10 IoT Enterprise LTSB 2016 64bit - **HMIPSP** on Windows 10 IoT Enterprise LTSB 2016 64bit - **PS-5711W, PS-5811W** on Windows 10 IoT Enterprise LTSB 2016 64bit - **HMIPSO** on Windows 10 IoT Enterprise LTSB 2016 64bit - **PS-5501W**, PS-5701W on Windows 10 IoT Enterprise LTSB 2016 64bit	Affected by: CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, CVE-2019-1223, CVE-2019-1224, CVE-2019-1225, CVE-2019-1226 *A fix is scheduled in December 2019* *The vulnerable service, Remote Desktop Services (RDS), is disabled by default on these products. Schneider Electric is currently validating the Microsoft patches.* *We advise customers not to enable RDS, or as a mitigation, to prevent access to this service from unauthorized sources.*
- **HMIG5U** on Windows Embedded Standard 7 with SP1 32bit - **PFXSP5B40** on Windows Embedded Standard 7 with SP1 32bit	Affected by: CVE-2019-1181, CVE-2019-1182 *The vulnerable service, Remote Desktop Services (RDS), is disabled by default on these products.* *We advise customers not to enable RDS, or as a mitigation, to prevent access to this service from unauthorized sources.* ***Note****: These products are no longer supported. Customers are encouraged to migrate to supported products.*
- **HMIG5U2, HMIG5UL8A, HMIG5UL8B** on Windows Embedded Standard 7 with SP1 32bit - **PFXSP5B41, PFXSP5B41S8A, PFXSP5B41S8B** on Windows Embedded Standard 7 with SP1 32bit	Affected by: CVE-2019-1181, CVE-2019-1182 *A fix is scheduled in December 2019* *The vulnerable service, Remote Desktop Services (RDS), is disabled by default on these products. Schneider Electric is currently validating the Microsoft patches. We advise customers not to enable RDS, or as a mitigation, to prevent access to this service from unauthorized sources.*

Schneider Electric Security Notification

Conext Control - Server **All versions**	Apply the following two Microsoft security patches to the Conext Control server: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
Version TGO_08.04.05-02_20190708 and prior TelevisGO (Eliwell)	Affected by: CVE-2019-1181, CVE-2019-1182 The vulnerabilities impact the Microsoft Windows Operating System of the BoxPC hosting the TelevisGo application. The vulnerable service, Remote Desktop Services (RDS), is disabled by default on all BoxPC manufactured after 15 July 2019. Schneider Electric has qualified the following patches which must be applied in the specified order below: 1. KB2592687 – Remote Desktop update to v8.0 2. KB4490628 – Dependency KB to be installed before DejaBlue security update 3. KB4512486 – DejaBlue security update These patches are now included in TelevisGo version TGO_08.04.05-03 integrated in the BoxPC. On the BoxPC, the automatic windows update is now activated by default.
All versions prior to September 2019 - **EcoStruxure Foxboro DCS** - **EcoStruxure Foxboro SCADA**	Affected by: CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, CVE-2019-1223, CVE-2019-1224, CVE-2019-1225, CVE-2019-1226 *Schneider Electric has successfully validated the Microsoft patches. The list of patches is available on https://pasupport.schneider-electric.com/content/Security/mspatch/mspatch.asp*

Schneider Electric Security Notification

General Security Recommendations

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

INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Appendix

Affected Product – including Operating System	Remediation
- **HMIBMU, HMIBMP** o Windows Embedded 8.1 Industry 64bit o Windows 7 Ultimate with SP1 64bit o Windows Embedded Standard 7 with SP1 64bit - **PS-5000 Modular Type (Core i7/Celeron Model)** o Windows Embedded 8.1 Industry 64bit o Windows 7 Ultimate with SP1 64bit - **PS-5000 Modular Type (Core i7/Celeron Model)** o Windows Embedded Standard 7 with SP1 64bit o Windows Embedded Standard 7 with SP1 32bit - **HMIPEP** o Windows Embedded 8.1 Industry 64bit o Windows 7 Ultimate with SP1 64bit o Windows Embedded Standard 7 with SP1 64bit - **PS-5821W** o Windows Embedded 8.1 Industry 64bit o Windows 7 Ultimate with SP1 64bit o Windows Embedded Standard 7 with SP1 64bit o Windows Embedded Standard 7 with SP1 32bit - **HMIPSP** o Windows Embedded 8.1 Industry 64bit o Windows 7 Ultimate with SP1 64bit o Windows Embedded Standard 7 with SP1 64bit - **PS-5711W, PS-5811W** o Windows Embedded 8.1 Industry 64bit o Windows 7 Ultimate with SP1 64bit	Affected by: CVE-2019-1181, CVE-2019-1182 *The vulnerable service, Remote Desktop Services (RDS), is disabled by default on these products. Schneider Electric is currently validating the Microsoft patches.* *We advise customers not to enable RDS, or as a mitigation, to prevent access to this service from unauthorized sources.*

○ Windows Embedded Standard 7 with SP1 64bit ○ Windows Embedded Standard 7 with SP1 32bit - **HMIPSO** ○ Windows Embedded 8.1 Industry 64bit ○ Windows 7 Ultimate with SP1 64bit ○ Windows Embedded Standard 7 with SP1 64bit - **PS-5501W, PS-5701W** ○ Windows Embedded 8.1 Industry 64bit ○ Windows 7 Ultimate with SP1 64bit ○ Windows Embedded Standard 7 with SP1 64bit ○ Windows Embedded Standard 7 with SP1 32bit - **HMIPP** ○ Windows 7 Ultimate with SP1 64bit ○ Windows 7 Ultimate with SP1 32bit ○ Windows Embedded Standard 7 with SP1 32bit - **PS-4600 (Core i3)** ○ Windows 7 Ultimate with SP1 64bit ○ Windows 7 Ultimate with SP1 32bit ○ Windows Embedded Standard 7 with SP1 32bit - **HMIPU** ○ Windows 7 Ultimate with SP1 64bit ○ Windows 7 Ultimate with SP1 32bit ○ Windows Embedded Standard 7 with SP1 32bit - **PS-4600 (Celeron)** ○ Windows 7 Ultimate with SP1 64bit ○ Windows 7 Ultimate with SP1 32bit ○ Windows Embedded Standard 7 with SP1 32bit - **HMIBSU** ○ Windows Embedded Standard 7 with SP1 32bit - **PE-4000B (N2600)** ○ Windows Embedded Standard 7 with SP1 32bit - **HMIRSP** ○ Windows Server 2012 R2 ○ Windows Server 2008 Standard R2 ○ Windows 7 Ultimate with SP1 64bit - **HMIRXO** ○ Windows 7 Ultimate with SP1 64bit - **HMIRSO** ○ Windows 7 Ultimate with SP1 64bit - **HMIRSU** ○ Windows 7 Ultimate with SP1 64bit	Affected by: CVE-2019-1181, CVE-2019-1182 *The vulnerable service, Remote Desktop Services (RDS), is disabled by default on these products. Schneider Electric is currently validating the Microsoft patches.* *We advise customers not to enable RDS, or as a mitigation, to prevent access to this service from unauthorized sources.*

- **HMIBP**
  ○ Windows 7 Ultimate with SP1 64bit
  ○ Windows 7 Ultimate with SP1 32bit
  ○ Windows Embedded Standard 7 with SP1 32bit
- **PS-4000B (P8400)**
  ○ Windows 7 Ultimate with SP1 64bit
  ○ Windows 7 Ultimate with SP1 32bit
  ○ Windows Embedded Standard 7 with SP1 32bit
- **HMIBU**
  ○ Windows 7 Ultimate with SP1 32bit
  ○ Windows Embedded Standard 7 with SP1 32bit
- **PS-4000B (N270)**
  ○ Windows 7 Ultimate with SP1 32bit
  ○ Windows Embedded Standard 7 with SP1 32bit
- **PS-4700, PS-4800 (P8400)**
  ○ Windows 7 Ultimate with SP1 64bit
  ○ Windows 7 Ultimate with SP1 32bit
  ○ Windows Embedded Standard 7 with SP1 32bit
- **PS-4700, PS-4800 (N270)**
Windows 7 Ultimate with SP1 32bit Windows Embedded Standard 7 with SP1 32bit
	Affected by: CVE-2019-1181, CVE-2019-1182
	The vulnerable service, Remote Desktop Services (RDS), is disabled by default on these products. Schneider Electric is currently validating the Microsoft patches.
	We advise customers not to enable RDS, or as a mitigation, to prevent access to this service from unauthorized sources.

Revision Control:

Version 1.0 *24 Sep 2019*	Original Release
Version 2.0 *12 Nov 2019*	Updated affected products to include *EcoStruxure Technology Platform (ETP)* (page 4), updated remediation for *EcoStruxure Substation Operation Gateway* (page 4), and updated the affected product details for *Conext Control* (page 6).
Version 3.0 *26 Nov 2019*	Updated Remediation for *Version TGO_08.04.05-02_20190708 and prior TelevisGO (Eliwell)* (page 6)
Version 4.0 *14 Jan 2020*	Updated fixed version information for *TelevisGO (Eliwell)* (page 6) Updated Remediation for EcoStruxure Foxboro DCS and EcoStruxure Foxboro SCADA (page 7)
Version 5.0 *12 Oct 2021*	Added remediations for *Conext™ Advisor 2 Cloud, Conext™ Advisor 2 Gateway*, *Conext™ Control V2 Gateway* (page 3)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.10.11 11:57:55 -04'00'