Schneider Electric Security Bulletin

Microsoft Remote Desktop Services – DejaBlue (V1.2)

16 August 2019 (19 August 2019)

Overview

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 Microsoft's security updates webpage for further information and guidance for any affected systems. As a recommended mitigation by Microsoft, customers can consider disabling Remote Desktop Services if they are not required.

Details

The four vulnerabilities corresponding to CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, and CVE-2019-1226 could potentially lead to remote-code execution. An unauthenticated attacker could connect to the target system using Remote Desktop Protocol (RDP) and send specially crafted requests to install or delete programs, create user accounts, etc.

Two of the remote code execution vulnerabilities (dubbed 'DejaBlue' by security researchers), CVE-2019-1181 and CVE-2019-1182, are 'wormable', meaning that any future malware that exploits these could propagate from vulnerable computer to vulnerable computer without any user interaction.

The two vulnerabilities corresponding to CVE-2019-1224 and CVE-2019-1225 can lead to information disclosure. An attacker could gain access to confidential information as the server improperly discloses the contents of its memory when this vulnerability is exploited.

The vulnerability corresponding to CVE-2019-1223 is a Denial-of-Service vulnerability which allows an attacker to send specially crafted packets to RDP service, which causes it to stop responding.

Recommended Mitigations

Please note that as of the date of this publication, it is unclear how Microsoft's patches and updates will affect systems performance. Therefore, 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.

Schneider Electric continues to monitor and track research into these vulnerabilities to determine appropriate actions to be taken. We advise customers to refer immediately to the following specific Microsoft security update resources for further information and guidance.

https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/

Remote-code execution vulnerabilities:

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

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226

Information disclosure vulnerabilities:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1224

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1225

Denial-of-Service vulnerability:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1223

General Security Recommendations

We strongly recommend applying the following industry cybersecurity best practices:

- 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.

More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it.

To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative or your Customer Care Center: https://www.schneider-electric.com/en/work/support/contacts.jsp. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric’s products, please visit the company’s cybersecurity web page: http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

If you require additional support, Schneider Electric Industrial Cybersecurity Services team is available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN “AS-IS” BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Schneider Electric Security Bulletin

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 **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 *16-Aug-2019*	Original Release
Version 1.1 *16-Aug-2019*	- Added recommended mitigation to (page 1)
Version 1.2 *19-Aug-2019*	- Updated Legal Disclaimer (page 3)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.08.19 17:44:14 -04'00'