Schneider Electric Security Bulletin V1.1
CVE-2019-0708 Microsoft Remote Desktop Services (BlueKeep)

16 May 2019 (10 September 2019)

Overview

Update: Schneider Electric is aware of an exploit available that targets the BlueKeep vulnerability. Our customers should urgently consider applying the detailed in the Microsoft Remote Desktop Services (BlueKeep) Security Notification document - https://www.schneider-electric.com/en/download/document/SEVD-2019-193-02/

Schneider Electric is aware of a Remote Desktop Services (RDS) vulnerability in a wide range of Microsoft operating systems, including Microsoft XP, Windows 7, Server 2003, and Server 2008 and 2008R2. Windows 8 and Windows 10 are not affected. If exploited, the remote-code execution 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. Schneider Electric continues to assess how the RDS vulnerability impacts our offers. In the meantime, we advise customers to refer immediately to Microsoft's security updates webpage for further information and guidance.

Details

The RDS vulnerability affects desktop, laptop, thin clients, and virtual computers. Microsoft officials say this vulnerability is pre-authentication and requires no user interaction, i.e., any malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer.

While programs normally only see their own data, a malicious program that exploits the RDS vulnerability would use internal memory buffers to obtain secrets currently processed by other running programs. These secrets could be user-level secrets, such as browser history, website content, user keys, and passwords, or system-level secrets, such as disk encryption keys.

CVE-2019-0708 is the official vulnerability references for the RDS vulnerability.

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.

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 to determine appropriate actions to be taken. We advise customers to refer immediately to Microsoft's security updates webpage for further information and guidance.

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

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

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 to prevent unauthorized access to the ICS and safety controllers, peripheral equipment and 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 are 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 these networks might have vulnerabilities and therefore 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 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

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. 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 May 2019*	Original Release
Version 1.1 *10 September 2019*	Exploit information added to Overview Section (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.09.09 23:13:50 -04'00'