Schneider Electric Security Notification

Conext™ Advisor & Conext™ Control V2

12 October 2021

Overview

Schneider Electric is aware of multiple Microsoft Windows vulnerabilities in its Schneider Conext™ Advisor 2 & Conext™ Control V2 products.

The Conext™ Advisor 2 is a web portal with an efficient, task-oriented interface for managing and optimizing the performance of solar power plants and includes a complete suite of tools for professional users.

The Conext™ Control V2 is a Solar Power Plant monitoring solution.

Failure to apply the remediations provided below may risk remote code execution, which could result in undesired behavior within the operating system. An attacker who successfully exploits this vulnerability could execute arbitrary code on the target system and then install programs; view, change, or delete data; or create new accounts with full user rights.

Affected Products and Versions

Product	Version
Conext™ Advisor 2 Cloud	2.02 and below
Conext™ Advisor 2 Gateway	1.28.45 and below
Conext™ Control V2 Gateway	2.6 and below

Vulnerability Details

CVE ID: **CVE-2019-11135**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.

CVE ID: **CVE-2020-0601**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source, aka 'Windows CryptoAPI Spoofing Vulnerability'.

CVE ID: **CVE-2020-0609**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0610.

CVE ID: **CVE-2020-0610**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0609.

CVE ID: **CVE-2020-0796**

CVSS v3.1 Base Score 10 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

CVE ID: **CVE-2020-0938**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1020.

CVE ID: **CVE-2020-1020**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely, aka 'Adobe Font Manager Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0938.

CVE ID: **CVE-2020-1350**

CVSS v3.1 Base Score 10 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka 'Windows DNS Server Remote Code Execution Vulnerability'.

CVE ID: **CVE-2020-1472**

CVSS v3.1 Base Score 10 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

CVE ID: **CVE-2019-0803**

CVSS v3.0 Base Score 7.8 | High | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859.

CVE ID: **CVE-2019-1040**

CVSS v3.0 Base Score 5.9 | Medium | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.

Remediation

Version Windows 10 of the Microsoft Windows includes a fix for this vulnerability and is available for download here:

Affected Product & Version	Remediation
Conext™ Advisor 2 Cloud	• https://www.microsoft.com/en-in/software-download/windows10 • Reboot is required
Conext™ Advisor 2 Gateway	• https://www.microsoft.com/en-in/software-download/windows10 • Reboot is required
Conext™ Control V2 Gateway	• https://www.microsoft.com/en-in/software-download/windows10 • Reboot is required

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

Schneider Electric Security Notification

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric’s products, visit the company’s cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Notification

SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. 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 1.0 *12 October 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.10.10 02:21:48 -04'00'