Schneider Electric Security Notification

EcoStruxure™ Operator Terminal Expert (Vijeo XD) (V3.0)

12 May 2020 (10 November 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities in the EcoStruxure™ Operator Terminal Expert product (formerly known as Vijeo XD).

The EcoStruxure™ Operator Terminal Expert product is a configuration software for Harmony ranges supporting gestures and UI designs.

Failure to apply the remediations provided below may risk unauthorized command execution by a local user of the Windows engineering workstation, which could result in loss of availability, confidentiality and integrity of the workstation when running EcoStruxure™ Operator Terminal Expert.

November 2020 update: Fixes for CVE-2020-7495 and CVE-2020-7497 are available in EcoStruxure™ Operator Terminal Expert version 3.1 Service Pack 1B. This set of fixes supercedes Service Pack 1A which should be upgraded to 1B.

Affected Products and Versions

Product & Version	Affected by
EcoStruxure™ Operator Terminal Expert 3.1 Service Pack 1A and prior (formerly known as Vijeo XD)	CVE-2020-7495 CVE-2020-7497
EcoStruxure™ Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD)	CVE-2020-7493 CVE-2020-7494 CVE-2020-7496

Vulnerability Details

CVE ID: **CVE-2020-7493**

CVSS v3.0 Base Score 7.7 | High | CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

A CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists which could cause malicious code execution when opening the project file.

CVE ID: **CVE-2020-7494**

CVSS v3.0 Base Score 7.7 | High | CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists which could cause malicious code execution when opening the project file.

CVE ID: **CVE-2020-7495**

CVSS v3.0 Base Score 3.3 | Low | CVSS:3.0/ AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability during zip file extraction exists which could cause unauthorized write access outside of expected path folder when opening the project file.CVE ID: **CVE-2020-7496**

CVE ID: **CVE-2020-7496**

CVSS v3.0 Base Score 3.3 | Low | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

A CWE-88: Argument Injection or Modification vulnerability exists which could cause unauthorized write access when opening the project file.

CVE ID: **CVE-2020-7497**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H

A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists which could cause arbitrary application execution when the computer starts.

Remediation

These vulnerabilities are fixed in the EcoStruxure™ Operator Terminal Expert 3.1 Service Pack 1B. Service Pack 1A is now superceded by Service Pack 1B and should be upgraded using the link below:

https://www.se.com/ww/en/product-range-download/62621-ecostruxure%E2%84%A2-operator-terminal-expert/#/software-firmware-tab

The fix is also available through Schneider Electric Software Update (SESU).

We strongly recommend users to apply the listed mitigations in addition to the General Security Recommendations listed below.

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 for the devices that it is intended for.
- 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 laptops 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.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2020-7493	Steven Seeley and Chris Anastasio of Incite Team working with TrendMicro's Zero Day Initiative
CVE-2020-7494, CVE-2020-7496	Sharon Brizinov, Amir Preminger of Claroty Research working with TrendMicro's Zero Day Initiative
CVE-2020-7495	Sharon Brizinov, Amir Preminger of Claroty Research working with TrendMicro's Zero Day Initiative Fredrik Østrem (Cognite), Emil Sandstø (Cognite), and Cim Stordal (Cognite)
CVE-2020-7497	Fredrik Østrem (Cognite), Emil Sandstø (Cognite), and Cim Stordal (Cognite)

Schneider Electric Security Notification

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

About Schneider Electric

At Schneider, we believe **access to energy and digital resources** 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 digital automation** 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

Schneider Electric Security Notification

Revision Control:

Version 1.0 *12 May 2020*	Original Release
Version 2.0 *09 June 2020*	Update of CVE-2020-7495: this vulnerability is partially fixed in EcoStruxure™ Operator Terminal Expert version 3.1 Service Pack 1A and requires additional mitigation to reduce the risk (page 2)
Version 3.0 *10 November 2020*	Fix for CVE-2020-7495 & CVE-2020-7497 are available in EcoStruxure™ Operator Terminal Expert version 3.1 Service Pack 1B (page 2)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.11.08 20:42:31 -05'00'