Schneider Electric Security Notification

Security Notification – U.motion Builder software (V1.2)

5 April 2018 (11 Feb 2020)

Overview

Schneider Electric is aware of an exploit that targets Schneider Electric's U.motion Builder software. It is imperative customers cease using U.motion Builder software and remove it from their systems immediately.

Affected Product(s)

U.motion Builder Software, all versions prior to v1.3.4

Vulnerability Details

CVE ID: **CVE-2018-7763**

4.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Css.inc Directory Traversal Information Disclosure

The vulnerability exists within css.inc.php. The 'css' parameter contains a directory traversal vulnerability.

CVE ID: **CVE-2018-7764**

4.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

runscript Directory Traversal Information Disclosure

The vulnerability exists within runscript.php applet. There is a directory traversal vulnerability in the processing of the 's' parameter of the applet.

CVE ID: **CVE-2018-7765**

8.8| (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

track_import_export SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of track_import_export.php. The underlying SQLite database query is subject to SQL injection on the object_id input parameter.

CVE ID: **CVE-2018-7766**

6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

track_getdata SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of track_getdata.php. The underlying SQLite database query is subject to SQL injection on the id input parameter.

CVE ID: **CVE-2018-7767**

6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

editobject SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of the editobject.php. The underlying SQLite database query is subject to SQL injection on the type input parameter.

CVE ID: **CVE-2018-7768**

6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

loadtemplate SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of loadtemplate.php. The underlying SQLite database query is subject to SQL injection on the tpl input parameter.

CVE ID: **CVE-2018-7769**

6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

xmlserver SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of xmlserver.php. The underlying SQLite database query is subject to SQL injection on the id input parameter.

Schneider Electric Security Notification

CVE ID: **CVE-2018-7770**

6.5 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

sendmail email_attachment Parameter Absolute Path Traversal Information Disclosure Vulnerability

The vulnerability exists within processing of sendmail.php. The applet allows callers to select arbitrary files to send to an arbitrary email address.

CVE ID: **CVE-2018-7771**

5.5 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L

editscript Directory Traversal Remote Code Execution Vulnerability

The vulnerability exists within processing of editscript.php. A directory traversal vulnerability allows a caller with standard user privileges to write arbitrary php files anywhere in the web service directory tree.

CVE ID: **CVE-2018-7772**

6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

HTTP Cookie SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of applets which are exposed on the web service. The underlying SQLite database query to determine whether a user is logged in is subject to SQL injection on the loginSeed parameter, which can be embedded in the HTTP cookie of the request.

CVE ID: **CVE-2018-7773**

6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

nfcserver SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of nfcserver.php. The underlying SQLite database query is subject to SQL injection on the sessionid input parameter.

CVE ID: **CVE-2018-7774**

6.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

localize SQL Injection Remote Code Execution Vulnerability

The vulnerability exists within processing of localize.php. The underlying SQLite database query is subject to SQL injection on the username input parameter.

CVE ID: **CVE-2018-7776**

4.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Error Information Disclosure Vulnerability

The vulnerability exists within error.php. System information is returned to the attacker that contains sensitive data.

CVE ID: **CVE-2018-7777**

8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Remote Code Execution

The vulnerability is due to insufficient handling of update_file request parameter on update_module.php. A remote, authenticated attacker can exploit this vulnerability by sending a crafted request to the target server.

CVE ID: **CVE-2017-7494**

4.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Samba Cry - Malicious clients can upload and cause the smbd server to execute a shared library from a writable share.

Remediation

To further protect their installations from this threat, customers should immediately remove the U.motion Builder software from their systems.

The product has been retired and is no longer available or supported.

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.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for all efforts related to identifying and coordinating a response to this vulnerability:

CVE	Researcher Name
CVE-2018 7763, CVE-2018-7764, CVE-2018-7765, CVE-2018-7766, CVE-2018-7767, CVE-2018-7768, CVE-2018-7769, CVE-2018-7770, CVE-2018-7771, CVE-2018-7772, CVE-2018-7773, CVE-2018-7774, CVE-2018-7776	Rgod via ZDI
CVE-2018-7777	Constantin-Cosmin Craciun

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** 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

Schneider Electric Security Notification

Revision Control:

Version 1 *05 April 2018*	Original Release
Version 1.1 *19 April 2018*	Removed CVE-2018-7775 as it is a duplicate of CVE-2017-9960
Version 1.2 *11 February 2020*	Updated remediation section and overview section

Product Security Office

Digitally signed by Product Security Office
Date: 2020.02.11 16:07:24 -05'00'