Security Notification – U.motion Builder V1.1

05-Apr-2018 (Updated 19-Apr-2018)

Overview

Schneider Electric has become aware of multiple vulnerabilities in the U.motion Builder software.

Vulnerability Overview

The vulnerabilities identified are:

1. css_inc Directory Traversal Information Disclosure
2. runscript Directory Traversal Information Disclosure
3. track_import_export SQL Injection RCE
4. track_getdata_php SQL Injection RCE
5. editobject_php SQL Injection RCE
6. loadtemplate_php SQL Injection RCE
7. xmlserver SQL Injection RCE
8. sendmail email_attachment Parameter Absolute Path Traversal Information Disclosure
9. editscript Path Traversal RCE
10. HTTP Cookie SQL Injection RCE
11. nfcserver SQL Injection RCE
12. localize SQL Injection RCE
13. error Information Disclosure
14. Remote Code Execution
15. Samba-Remote Code Execution

Product(s) Affected

The product affected:

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

Vulnerability Details

1. Css.inc Directory Traversal Information Disclosure
   The vulnerability exists within css.inc.php. The 'css' parameter contains a directory traversal vulnerability.

   Overall CVSS Score: 4.3

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

   CVE ID: CVE-2018-7763

2. 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.

   Overall CVSS Score: 4.3

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

   CVE ID: CVE-2018-7764

3. 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.

   Overall CVSS Score: 8.8

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE ID: CVE-2018-7765

4. 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.

   Overall CVSS Score: 6.3

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

   CVE ID: CVE-2018-7766

5. 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.

   Overall CVSS Score: 6.3

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

CVE ID: CVE-2018-7767

6. 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.

   Overall CVSS Score: 6.3

   (CVSS V3 Vector):CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

   CVE ID: CVE-2018-7768

7. 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.

   Overall CVSS Score: 6.3

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

   CVE ID: CVE-2018-7769

8. 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.

   Overall CVSS Score: 6.5

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

   CVE ID: CVE-2018-7770

9. 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.

   Overall CVSS Score: 5.5

   (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L

   CVE ID: CVE-2018-7771

10. 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

Overall CVSS Score: 6.3

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

CVE ID: CVE-2018-7772

11. 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

    Overall CVSS Score: 6.3

    (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

    CVE ID: CVE-2018-7773

12. 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

    Overall CVSS Score: 6.3

    (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

    CVE ID: CVE-2018-7774

13. Error Information Disclosure Vulnerability
    The vulnerability exists within error.php. System information is returned to the attacker that contains sensitive data.

    Overall CVSS Score: 4.3

    (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

    CVE ID: CVE-2018-7776

14. 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.

    Overall CVSS Score: 8.8

    (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE ID: CVE-2018-7777

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

    Overall CVSS Score: 10.0

    (CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

    CVE ID: CVE-2017-7494

Mitigation

A fix for these vulnerabilities is available for download at:

https://www.schneider-electric.com/en/download/document/SE_UMOTION_BUILDER/

Schneider Electric recommends the following mitigations and best practices:

- Always place the machine running the U.motion Builder Software behind a robust firewall with carefully crafted rules to limit and control access.
- Never connect the machine directly to the Internet.
- Never place the machine in a DMZ.
- Never route Internet traffic directly to the machine.
- Remote access to the U.motion system should be conducted only over a trusted VPN.
- Limit connection to the U.motion Builder Software only to trusted machines with a legitimate need to connect.
- Utilize application whitelisting to limit what can run on the machine running the U.motion builder software.
- Utilize access control features available in the native *Windows Firewall* as detailed in the Microsoft Knowledge Base (e.g. http://technet.microsoft.com/en-us/library/cc725770%28WS.10%29.aspx).

Acknowledgements

Schneider Electric would like to thank the following for their identification of these vulnerabilities:

Rgod via ZDI:

- 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

Constantin-Cosmin Craciun

- CVE-2018-7777

For 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. 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

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

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

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2018.04.19 08:48:49 -04'00'