



CVE-2018-7831

Published on: 11/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:39 PM UTC

CVE-2018-7831

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Modicom Bmxnor0200h](#) from [Schneider-electric](#) contain the following vulnerability:

An Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability exists in the embedded web servers in all Modicon M340, Premium, Quantum PLCs and BMXNOR0200 allowing an attacker to send a specially crafted URL to a currently authenticated web server user to execute a password change on the

web server.

CVE-2018-7831 has been assigned by cybersecurity@schneider-electric.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Schneider Electric SE - Embedded Web Servers in all Modicon M340, Premium, Quantum PLCs and BMXNOR0200 version Embedded Web Servers in all Modicon M340, Premium, Quantum PLCs and BMXNOR0200**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[R1] Multiple Schneider Electric Modicon Quantum Vulnerabilities - Research Advisory Tenable®	Exploit Third Party Advisory www.tenable.com text/html	 MISC www.tenable.com/security/research/tra-2018-38
Security Notification - Embedded Web Servers for Modicon (V3.2) Schneider Electric	Vendor Advisory www.schneider-electric.com text/html	 CONFIRM www.schneider-electric.com/en/download/document/SEVD-2018-327-01/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

590900 Schneider Electric Embedded Web Servers for Modicon Multiple Vulnerabilities (SEVD-2018-327-01)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Schneider-electric	Modicom Bmxnor0200h	-	All	All	All
Hardware 	Schneider-electric	Modicom Bmxnor0200h	-	All	All	All
Operating System	Schneider-electric	Modicom Bmxnor0200h Firmware	All	All	All	All
Operating System	Schneider-electric	Modicom Bmxnor0200h Firmware	All	All	All	All
Hardware 	Schneider-electric	Modicom M340	-	All	All	All
Hardware 	Schneider-electric	Modicom M340	-	All	All	All
Operating System	Schneider-electric	Modicom M340 Firmware	All	All	All	All
Operating System	Schneider-electric	Modicom M340 Firmware	All	All	All	All
Hardware 	Schneider-electric	Modicom Premium	-	All	All	All
Hardware 	Schneider-electric	Modicom Premium	-	All	All	All
Operating System	Schneider-electric	Modicom Premium Firmware	All	All	All	All
Operating System	Schneider-electric	Modicom Premium Firmware	All	All	All	All
Hardware 	Schneider-electric	Modicom Quantum	-	All	All	All
Hardware 	Schneider-electric	Modicom Quantum	-	All	All	All
Operating System	Schneider-electric	Modicom Quantum Firmware	All	All	All	All
Operating System	Schneider-electric	Modicom Quantum Firmware	All	All	All	All

system

```
cpe:2.3:h:schneider-electric:modicom_bmxnor0200h:-:*:*:*:*:*:
```

```
cpe:2.3:h:schneider-electric:modicom_bmxnor0200h:-:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:schneider-electric:modicom_bmxnor0200h_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:schneider-electric:modicom m340:-:*:*:*:*:*:
```

```
cpe:2.3:h:schneider-electric:modicom m340:-:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:o:schneider-electric:modicom_m340_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:schneider-electric:modicom_premium:-:*:*:*:*:*:
```

```
cpe:2.3:h:schneider-electric:modicom_premium:-:*:*:*:*:*:
```

```
cpe:2.3:o:schneider-electric:modicom premium firmware:*.~*~*~*~*~*~*~*~*~*
```

```
cpe:2.3:o:schneider-electric:modicom premium firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:schneider-electric:modicom_quantum:-:*:*:*:*:*:
```

```
cpe:2.3:h:schneider-electric:modicom_quantum:-:*:*:*:*:*:
```

```
cpe:2.3:o:schneider-electric:modicom quantum firmware:*.:.:.:.:.:.:.:.:
```

```
cpe:2.3:o:schneider-electric:modicom quantum firmware:*.*.*.*.*.*.*.*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report