



# CVE-2018-7833

Published on: 12/17/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

## CVE-2018-7833

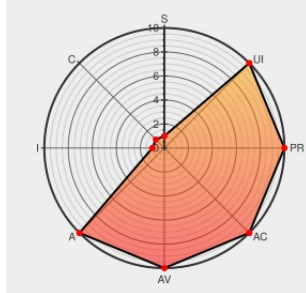
[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

An Improper Check for Unusual or Exceptional Conditions vulnerability exists in the embedded web servers in all Modicon M340, Premium, Quantum PLCs and BMXNOR0200 where an unauthenticated user can send a specially crafted XML data via a POST request to cause the web server to become unavailable

CVE-2018-7833 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: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description | Tags | Link |
|-------------|------|------|
|-------------|------|------|

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](mailto: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    | <a href="#">Schneider-electric</a> | <a href="#">Modicom Bmxnor0200h</a>          | -       | All    | All     | All      |
| Hardware    | <a href="#">Schneider-electric</a> | <a href="#">Modicom Bmxnor0200h</a>          | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom Bmxnor0200h Firmware</a> | All     | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom Bmxnor0200h Firmware</a> | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Modicom M340</a>                 | -       | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Modicom M340</a>                 | -       | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom M340 Firmware</a>        | All     | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom M340 Firmware</a>        | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Modicom Premium</a>              | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Modicom Premium</a>              | All     | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom Premium Firmware</a>     | All     | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom Premium Firmware</a>     | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Modicom Quantum</a>              | All     | All    | All     | All      |
| Hardware  | <a href="#">Schneider-electric</a> | <a href="#">Modicom Quantum</a>              | All     | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom Quantum Firmware</a>     | All     | All    | All     | All      |
| Operating System                                                                             | <a href="#">Schneider-electric</a> | <a href="#">Modicom Quantum Firmware</a>     | All     | All    | All     | All      |

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: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: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](https://status.cve.report)