



# CVE-2020-7541

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2020-7541
<b>State</b>	PUBLIC
<b>Assigner</b>	cybersecurity@schneider-electric.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-11 01:15:00 UTC
<b>Updated</b>	2020-12-14 21:07:00 UTC
<b>Description</b>	A CWE-425: Direct Request ('Forced Browsing') vulnerability exists in the Web Server on Modicon M340, Legacy Offers Mc

## Risk And Classification

**Problem Types:** CWE-425

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Schneider-electric</a>	140cpu65150	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140cpu65150	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140cpu65150 Firmware	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140cpu65150 Firmware	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140noc77101	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140noc77101	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140noc77101 Firmware	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140noc77101 Firmware	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140noc78000	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140noc78000	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140noc78000 Firmware	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140noc78000 Firmware	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140noc78100	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140noc78100	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140noc78100 Firmware	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	140noc78100 Firmware	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	140noe77111	-	All	All	All

Hardware	Schneider-electric	140noe77111	-	All	All	All
Operating System	Schneider-electric	140noe77111 Firmware	All	All	All	All
Operating System	Schneider-electric	140noe77111 Firmware	All	All	All	All
Hardware	Schneider-electric	Bmxnoc0401	-	All	All	All
Hardware	Schneider-electric	Bmxnoc0401	-	All	All	All
Operating System	Schneider-electric	Bmxnoc0401 Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxnoc0401 Firmware	All	All	All	All
Hardware	Schneider-electric	Bmxnoe0100	-	All	All	All
Hardware	Schneider-electric	Bmxnoe0100	-	All	All	All
Operating System	Schneider-electric	Bmxnoe0100 Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxnoe0100 Firmware	All	All	All	All
Hardware	Schneider-electric	Bmxnoe0110	-	All	All	All
Hardware	Schneider-electric	Bmxnoe0110	-	All	All	All
Operating System	Schneider-electric	Bmxnoe0110 Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxnoe0110 Firmware	All	All	All	All
Hardware	Schneider-electric	Bmxp341000	-	All	All	All
Hardware	Schneider-electric	Bmxp341000	-	All	All	All
Operating System	Schneider-electric	Bmxp341000 Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxp341000 Firmware	All	All	All	All
Hardware	Schneider-electric	Bmxp342000	-	All	All	All
Hardware	Schneider-electric	Bmxp342000	-	All	All	All
Operating System	Schneider-electric	Bmxp342000 Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxp342000 Firmware	All	All	All	All
Hardware	Schneider-electric	Bmxp3420102	-	All	All	All
Hardware	Schneider-electric	Bmxp3420102	-	All	All	All
Hardware	Schneider-electric	Bmxp3420102cl	-	All	All	All
Hardware	Schneider-electric	Bmxp3420102cl	-	All	All	All
Operating System	Schneider-electric	Bmxp3420102cl Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxp3420102cl Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxp3420102 Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxp3420102 Firmware	All	All	All	All
Hardware	Schneider-electric	Bmxp342020	-	All	All	All
Hardware	Schneider-electric	Bmxp342020	-	All	All	All
Operating System	Schneider-electric	Bmxp342020 Firmware	All	All	All	All
Operating System	Schneider-electric	Bmxp342020 Firmware	All	All	All	All

Hardware	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302cl</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302cl</a>	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302cl Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302cl Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302 Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Bmxxp3420302 Firmware</a>	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy4103</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy4103</a>	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy4103 Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy4103 Firmware</a>	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy5103</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy5103</a>	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy5103 Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxxy5103 Firmware</a>	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx574634</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx574634</a>	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx574634 Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx574634 Firmware</a>	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx575634</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx575634</a>	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx575634 Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx575634 Firmware</a>	All	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx576634</a>	-	All	All	All
Hardware	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx576634</a>	-	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx576634 Firmware</a>	All	All	All	All
Operating System	<a href="#">Schneider-electric</a>	<a href="#">Tsxpx576634 Firmware</a>	All	All	All	All

## References

### Reference

Security Notification - Web Server on Modicon M340, Legacy Offers Modicon Quantum and Modicon Premium and associated Communication

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

590745 Schneider Electric Web Server on Modicon M340 Legacy Offers Modicon Quantum and Modicon Premium and associated Communication Modules Multiple Vulnerabilities (SEVD-2020-343-03)

© [CVE.report](#) 2026 |

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](#)**