



CVE-2016-2278

Published on: 03/02/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:15 PM UTC

CVE-2016-2278

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

Certain versions of [Struxureware Building Operations Automation Server As](#) from [Schneider-electric](#) contain the following vulnerability:

Schneider Electric Struxureware Building Operations Automation Server AS 1.7 and earlier and AS-P 1.7 and earlier allows remote authenticated administrators to execute arbitrary OS commands by defeating an msh (aka Minimal Shell) protection mechanism.

CVE-2016-2278 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Schneider Electric SBO / AS - Multiple Vulnerabilities	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 39522

Schneider Electric Building Operation Automation
Server Vulnerability | ICS-CERT

Third Party Advisory
US Government Resource
ics-cert.us-cert.gov
text/html

 [MISC ics-cert.us-cert.gov/advisories/ICSA-16-061-01](https://ics-cert.us-cert.gov/advisories/ICSA-16-061-01)

Vendor Advisory
download.schneider-electric.com
application/pdf

 [CONFIRM download.schneider-electric.com/files?p_Doc_Ref=SEVD-2016-025-01](https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2016-025-01)

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

591226 Schneider Electric Building Operation Automation Server OS COMMAND INJECTION Vulnerability (ICSA-16-061-01, SEVD-2016-025-01)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Schneider-electric	Struxureware Building Operations Automation Server As	All	All	All	All
Hardware 	Schneider-electric	Struxureware Building Operations Automation Server As	All	All	All	All
Hardware 	Schneider-electric	Struxureware Building Operations Automation Server As-p	-	All	All	All
Hardware 	Schneider-electric	Struxureware Building Operations Automation Server As-p	-	All	All	All
Operating System	Schneider-electric	Struxureware Building Operations Automation Server As-p Firmware	1.7	All	All	All
Operating System	Schneider-electric	Struxureware Building Operations Automation Server As-p Firmware	1.7	All	All	All
Operating System	Schneider-electric	Struxureware Building Operations Automation Server As Firmware	All	All	All	All

cpe:2.3:h:schneider-electric:struxureware building operations automation server as:*.~*~*~*~*~*~*~*~*~*

cpe:2.3:h:schneider-electric:struxureware building operations automation server as:*.~.*.*.*.*.*.*.*.

cpe:2.3:h:schneider-electric:struxureware_building_operations_automation_server_as-p:-:*:*:*:*:*:

cpe:2.3:h:schneider-electric:struxureware building operations automation server as-p:-:.*:.*:.*:.*:.*:.*

cpe:2.3:o:schneider-electric:struxureware building operations automation server as-p firmware:1.7:*:*:*:*:*:

cpe:2.3:o:schneider-electric:struxureware building operations automation server as-p firmware:1.7:*:*:*:*:*:

```
cpe:2.3:o:schneider-electric:struxureware building operations automation server as 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](#)