



CVE-2017-14459

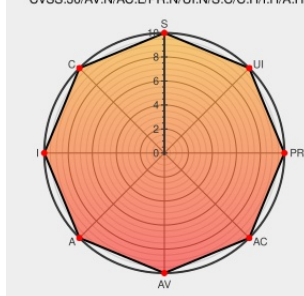
Published on: 04/11/2018 12:00:00 AM UTC

Last Modified on: 04/19/2022 07:15:00 PM UTC

CVE-2017-14459

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

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



Certain versions of [Awk-3131a](#) from [Moxa](#) contain the following vulnerability:

An exploitable OS Command Injection vulnerability exists in the Telnet, SSH, and console login functionality of Moxa AWK-3131A Industrial IEEE 802.11a/b/g/n wireless AP/bridge/client in firmware versions 1.4 to 1.7 (current). An attacker can inject commands via the username parameter of several services (SSH, Telnet, console), resulting in remote, unauthenticated, root-level operating system command execution.

CVE-2017-14459 has been assigned by [Cisco](#) talos-cna@cisco.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Cisco](#) Talos - Moxa version Moxa AWK-3131A Industrial IEEE 802.11a/b/g/n wireless AP/bridge/client versions 1.4 - 1.9. In addition, versions prior to 1.4 appear similarly vulnerable to injection, but not as easily exploitable (described below). Other models in the AWK product line may likewise be vulnerable but have not been tested.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

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.

591173 Moxa AWK-3131A Multiple Features Login Username Parameter OS Command Injection Vulnerability (TALOS-2017-0507)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Moxa	Awk-3131a	-	All	All	All
Hardware	Moxa	Awk-3131a	-	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.4	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.5	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.6	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.7	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.4	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.5	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.6	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.7	All	All	All

cpe:2.3:h:moxa:awk-3131a:-:*:*:*:*:*:

```
cpe:2.3:o:moxa:awk-3131a_firmware:1.4.*:*:*:*:*:
```

```
cpe:2.3:o:moxa:awk-3131a_firmware:1.5:*:*:*:*.*
```

```
cpe:2.3:o:moxa:awk-3131a_firmware:1.6:*:*:*:*.*
```

```
cpe:2.3:o:moxa:awk-3131a_firmware:1.7:*:*:*:*.*
```

```
cpe:2.3:o:moxa:awk-3131a_firmware:1.4:*****.*.*.
```

cpe:2.3:o:moxa:awk-3131a_firmware:1.5:*****:

cpe:2.3:o:moxa:awk-3131a_firmware:1.6:*****:

cpe:2.3:o:moxa:awk-3131a_firmware:1.7:*****:

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](#)