



CVE-2016-8721

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-8721
State	PUBLISHED
Assigner	talos
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-20 18:59:01 UTC
Updated	2025-04-20 01:37:25 UTC
Description	An exploitable OS Command Injection vulnerability exists in the web application 'ping' functionality of Moxa AWK-3131A Wi

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Problem Types: CWE-78 | remote code execution

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.0	talos-cna@cisco.com	Secondary	9.1	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.0	CNA	DECLARED	9.1	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9		AV:N/AC:L/Au:S/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Complete

ntegrity

Complete

Availability

Complete

AV:N/AC:L/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Moxa	Awk-3131a	-	All	All	All
Operating System	Moxa	Awk-3131a Firmware	1.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Moxa	Moxa AWK-3131A WAP	affected 1.1 Build 15122211	Not specified

References

Reference	Source	Link	Tags
Cisco Talos - Talos 2016 0235	af854a3a-2127-422b-91ae-364da2661108	www.talosintelligence.com	Exploit, Technical Description, Thi
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.