CVE-2015-7323

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

Summary

CVE	CVE-2015-7323
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-05 15:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Secure Meeting (Pulse Collaboration) in Pulse Connect Secure (formerly Juniper Junos Pulse) before 7.1R22.1, 7.4, 8.

Risk And Classification

Primary CVSS: v2.0 3.5 from nvd@nist.gov

AV:N/AC:M/Au:S/C:P/I:N/A:N

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:S/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Juniper	Pulse Connect Secure	7.1	All	All	All

Application	Juniper	Pulse Connect Secure	7.4	All	All	All
Application	Juniper	Pulse Connect Secure	8.0	All	All	All
Application	Juniper	Pulse Connect Secure	8.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
profundis-labs.com/advisories/CVE-2015-7323.txt
Junos Pulse Secure Meeting 8.0.5 Access Bypass ≈ Packet Storm
Pulse Connect Secure Access Control Flaw in Secure Meeting Component Lets Remote Authenticated Users Join Meetings on the Target Sy
Full Disclosure: CVE-2015-7323 - Secure Meeting (Pulse Collaboration) issue may allow authenticated users to bypass meeting authorization
Public KB - SA40054 - 2015-09: Security Advisory: Secure Meeting (Pulse Collaboration) issue may allow authenticated users to bypass meet
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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