CVE-2014-2107

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

Summary

CVE	CVE-2014-2107
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-27 21:55:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cisco IOS 12.2 and 15.0 through 15.3, when used with the Kailash FPGA before 2.6 on RSP720-3C-10GE and RSP720-3C

Risk And Classification

Primary CVSS: v2.0 7.1 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	12.2	All	All	All

Operating System	Cisco	Ios	15.0	All	All	All
Operating System	Cisco	Ios	15.0\(1\)se	All	All	All
Operating System	Cisco	Ios	15.1	All	All	All
Operating System	Cisco	Ios	15.2	All	All	All
Operating System	Cisco	Ios	15.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	So
Cisco Security Advisory: Cisco 7600 Series Route Switch Processor 720 with 10 Gigabit Ethernet Uplinks Denial of Service Vulnerability	af8
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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