CVE-2020-3118

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-3118
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-05 18:15:00 UTC
Updated	2022-12-23 16:59:00 UTC
Description	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, a

Risk And Classification

EPSS: 0.002560000 probability, percentile 0.489490000 (date 2026-04-01)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-787

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	IOS XR
Name	Cisco IOS XR Software Discovery Protocol Format String Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-3118

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 9000	-	All	All	All
Hardware	Cisco	Asr 9000v	-	All	All	All
Hardware	Cisco	Asr 9000v	-	All	All	All
Hardware	Cisco	Asr 9001	-	All	All	All
Hardware	Cisco	Asr 9001	-	All	All	All
Hardware	Cisco	Asr 9006	-	All	All	All
Hardware	Cisco	Asr 9006	-	All	All	All
Hardware	Cisco	Asr 9010	-	All	All	All

Hardware	Cisco	Asr 9010	-	All	All	All
Hardware	Cisco	Asr 9901	-	All	All	All
Hardware	Cisco	Asr 9901	-	All	All	All
Hardware	Cisco	Asr 9903	-	All	All	All
Hardware	Cisco	Asr 9904	-	All	All	All
Hardware	Cisco	Asr 9904	-	All	All	All
Hardware	Cisco	Asr 9906	-	All	All	All
Hardware	Cisco	Asr 9906	-	All	All	All
Hardware	Cisco	Asr 9910	-	All	All	All
Hardware	Cisco	Asr 9910	-	All	All	All
Hardware	Cisco	Asr 9912	-	All	All	All
Hardware	Cisco	Asr 9912	-	All	All	All
Hardware	Cisco	Asr 9920	-	All	All	All
Hardware	Cisco	Asr 9922	-	All	All	All
Hardware	Cisco	Asr 9922	-	All	All	All
Hardware	Cisco	Crs	-	All	All	All
Hardware	Cisco	Crs	-	All	All	All
Hardware	Cisco	Crs-x	-	All	All	All
Operating System	Cisco	Ios Xr	All	All	All	All
Operating System	Cisco	Ios Xr	5.2.5	All	All	All
Operating System	Cisco	Ios Xr	6.4.2	All	All	All
Operating System	Cisco	Ios Xr	6.5.2	All	All	All
Operating System	Cisco	Ios Xr	6.5.3	All	All	All
Operating System	Cisco	Ios Xr	6.6.25	All	All	All
Operating System	Cisco	Ios Xr	7.0.1	All	All	All
Operating System	Cisco	Ios Xr	All	All	All	All
Operating System	Cisco	Ios Xr	5.2.5	All	All	All
Operating System	Cisco	Ios Xr	6.5.2	All	All	All
Operating System	Cisco	Ios Xr	6.5.3	All	All	All
Operating System	Cisco	Ios Xr	6.6.25	All	All	All
Operating System	Cisco	Ios Xr	7.0.1	All	All	All
Hardware	Cisco	Ncs 1001	-	All	All	All
Hardware	Cisco	Ncs 1001	-	All	All	All
Hardware	Cisco	Ncs 1002	-	All	All	All
Hardware	Cisco	Ncs 1002	-	All	All	All

Hardware	Cisco	Ncs 1004	-	All	All	All
Hardware	Cisco	Ncs 1004	-	All	All	All
Hardware	Cisco	Ncs 5001	-	All	All	All
Hardware	Cisco	Ncs 5001	-	All	All	All
Hardware	Cisco	Ncs 5002	-	All	All	All
Hardware	Cisco	Ncs 5002	-	All	All	All
Hardware	Cisco	Ncs 5011	-	All	All	All
Hardware	Cisco	Ncs 5011	-	All	All	All
Hardware	Cisco	Ncs 520	-	All	All	All
Hardware	Cisco	Ncs 520	-	All	All	All
Hardware	Cisco	Ncs 540	-	All	All	All
Hardware	Cisco	Ncs 540	-	All	All	All
Hardware	Cisco	Ncs 540-12z20g-sys-a	-	All	All	All
Hardware	Cisco	Ncs 540-12z20g-sys-a	-	All	All	All
Hardware	Cisco	Ncs 540-12z20g-sys-d	-	All	All	All
Hardware	Cisco	Ncs 540-12z20g-sys-d	-	All	All	All
Hardware	Cisco	Ncs 540-24z8q2c-sys	-	All	All	All
Hardware	Cisco	Ncs 540-24z8q2c-sys	-	All	All	All
Hardware	Cisco	Ncs 540-28z4c-sys-a	-	All	All	All
Hardware	Cisco	Ncs 540-28z4c-sys-a	-	All	All	All
Hardware	Cisco	Ncs 540-28z4c-sys-d	-	All	All	All
Hardware	Cisco	Ncs 540-28z4c-sys-d	-	All	All	All
Hardware	Cisco	Ncs 540-acc-sys	-	All	All	All
Hardware	Cisco	Ncs 540-acc-sys	-	All	All	All
Hardware	Cisco	Ncs 540l	-	All	All	All
Hardware	Cisco	Ncs 540l	-	All	All	All
Hardware	Cisco	Ncs 540x-12z16g-sys-a	-	All	All	All
Hardware	Cisco	Ncs 540x-12z16g-sys-a	-	All	All	All
Hardware	Cisco	Ncs 540x-12z16g-sys-d	-	All	All	All
Hardware	Cisco	Ncs 540x-12z16g-sys-d	-	All	All	All
Hardware	Cisco	Ncs 540x-16z4g8q2c-a	-	All	All	All
Hardware	Cisco	Ncs 540x-16z4g8q2c-a	-	All	All	All
Hardware	Cisco	Ncs 540x-16z4g8q2c-d	-	All	All	All
Hardware	Cisco	Ncs 540x-16z4g8q2c-d	-	All	All	All
Hardware	Cisco	Ncs 540x-acc-sys	-	All	All	All

Hardware	Cisco	Ncs 540x-acc-sys	-	All	All	All
Hardware	Cisco	Ncs 5501	-	All	All	All
Hardware	Cisco	Ncs 5501	-	All	All	All
Hardware	Cisco	Ncs 5501-se	-	All	All	All
Hardware	Cisco	Ncs 5501-se	-	All	All	All
Hardware	Cisco	Ncs 5502	-	All	All	All
Hardware	Cisco	Ncs 5502	-	All	All	All
Hardware	Cisco	Ncs 5502-se	-	All	All	All
Hardware	Cisco	Ncs 5502-se	-	All	All	All
Hardware	Cisco	Ncs 5508	-	All	All	All
Hardware	Cisco	Ncs 5508	-	All	All	All
Hardware	Cisco	Ncs 5516	-	All	All	All
Hardware	Cisco	Ncs 5516	-	All	All	All
Hardware	Cisco	Ncs 560	-	All	All	All
Hardware	Cisco	Ncs 560	-	All	All	All
Hardware	Cisco	Ncs 6000	-	All	All	All
Hardware	Cisco	Ncs 6000	-	All	All	All
Hardware	Cisco	Ncs 6008	-	All	All	All
Hardware	Cisco	Xrv 9000	-	All	All	All
Hardware	Cisco	Xrv 9000	-	All	All	All

References

Reference	Source	Link	Tags
Cisco IOS XR Software Cisco Discovery Protocol Format String Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
Cisco Discovery Protocol (CDP) Remote Device Takeover ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party Advisory,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report