CVE-2020-3153

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

Summary

CVE	CVE-2020-3153
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-19 20:15:00 UTC
Updated	2022-01-01 19:39:00 UTC
Description	A vulnerability in the installer component of Cisco AnyConnect Secure Mobility Client for Windows could allow an authentica

Risk And Classification

EPSS: 0.250870000 probability, percentile 0.961780000 (date 2026-04-14)

CISA KEV: Listed on 2022-10-24; due 2022-11-14; ransomware use Known

Problem Types: CWE-427

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	AnyConnect Secure
Name	Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ac-win-path-traverse-qO4HWBsj; https://nvd.nist.gov/vuln/detail/CVE-2020-3153

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All

References

Reference	Source	Link
Cisco AnyConnect Secure Mobility Client 4.8.01090 Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com
Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability	CISCO	tools.cisco.com
Cisco AnyConnect Path Traversal / Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com

Cisco AnyConnect Path Traversal / Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com
Cisco AnyConnect Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com
Full Disclosure: Cisco AnyConnect elevation of privileges due to insecure handling of path names	FULLDISC	seclists.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

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