



CVE-2023-20166

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-20166
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-18 03:15:00 UTC
Updated	2023-11-07 04:06:00 UTC
Description	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path travers

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine	3.2	-	All	All
Application	Cisco	Identity Services Engine	3.2	patch1	All	All

References

Reference	Source	Link	Tags
Cisco Identity Services Engine Path Traversal Vulnerabilities	CISCO	sec.cloudapps.cisco.com	
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.

Legacy QID Mappings

[317326](#) Cisco Identity Services Engine (ISE) Path Traversal Vulnerability (CVE-2023-20166) (cisco-sa-ise-traversal-ZTUgMYhu)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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