CVE-2023-20031

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

Summary

CVE	CVE-2023-20031
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-01 18:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the SSL/TLS certificate handling of Snort 3 Detection Engine integration with Cisco Firepower Threat Defe

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Firepower Threat Defense	6.7.0	All	All	All
Application	Cisco	Firepower Threat Defense	6.7.0.1	All	All	All
Application	Cisco	Firepower Threat Defense	6.7.0.2	All	All	All
Application	Cisco	Firepower Threat Defense	6.7.0.3	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.0	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.0.1	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.1	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.1.1	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.2	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.2.1	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.3	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.4	All	All	All
Application	Cisco	Firepower Threat Defense	7.0.5	All	All	All
Application	Cisco	Firepower Threat Defense	7.2.0	All	All	All
Application	Cisco	Firepower Threat Defense	7.2.0.1	All	All	All

References

Reference	Source	Link
Cisco Firepower Threat Defense Software SSL and Snort 3 Detection Engine Bypass and Denial of Service Vulnerability	MISC	sec.cl
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317395 Cisco Firepower Threat Defense (FTD) Software Secure Sockets Layer (SSL) and Snort 3 Detection Engine Bypass and Denial of Service (DoS) Vulnerability (cisco-sa-ftd-snort3-8U4HHxH8)