



CVE-2022-20746

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-20746 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-05-03 04:15:00 UTC |
| Updated | 2023-11-07 03:42:00 UTC |
| Description | A vulnerability in the TCP proxy functionality of Cisco Firepower Threat Defense (FTD) Software could allow an unauthentic |

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|--------------------------|---------|--------|---------|----------|
| Application | Cisco | Firepower Threat Defense | All | All | All | All |
| Application | Cisco | Firepower Threat Defense | 7.1.0 | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|---|---------------|
| 20220427 Cisco Firepower Threat Defense Software TCP Proxy Denial of Service Vulnerability | CISCO | tools.cisco.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, ar |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317170 Cisco Firepower Threat Defense (FTD) Software Transmission Control Protocol (TCP) Proxy Denial of Service (DoS) Vulnerability (cisco-sa-ftd-tcp-dos-kM9SHhOu)

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#).

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