CVE-2022-42472

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

Summary

CVE	CVE-2022-42472
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-16 19:15:00 UTC
Updated	2023-11-07 03:53:00 UTC
Description	A improper neutralization of crlf sequences in http headers ('http response splitting') in Fortinet FortiOS versions 7.2.0 throu

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	7.2.0	All	All	All
Operating System	Fortinet	Fortios	7.2.1	All	All	All
Operating System	Fortinet	Fortios	7.2.2	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All
Application	Fortinet	Fortiproxy	7.2.0	All	All	All
Application	Fortinet	Fortiproxy	7.2.1	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All
Application	Fortinet	Fortiproxy	All	All	All	All

References

Reference	Source	Link	Tags
PSIRT Advisories | FortiGuard	MISC	fortiguard.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

43985 FortiOS Header Injection In Proxy Vulnerability (FG-IR-22-362)

44044 FortiOS Header Injection In Proxy Vulnerability (FG-IR-22-362) (Unauthenticated Check)