CVE-2021-36173

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-36173
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-08 19:15:00 UTC
Updated	2021-12-10 16:37:00 UTC
Description	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 6

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Fortinet	Fortigate-1100e	-	All	All	All
Hardware	Fortinet	Fortigate-200f	-	All	All	All
Hardware	Fortinet	Fortigate-2600f	-	All	All	All
Hardware	Fortinet	Fortigate-3500f	-	All	All	All
Hardware	Fortinet	Fortigate-400e	-	All	All	All
Hardware	Fortinet	Fortigate-600e	-	All	All	All
Hardware	Fortinet	Fortigate 1800f	-	All	All	All
Hardware	Fortinet	Fortigate 2200e	-	All	All	All
Hardware	Fortinet	Fortigate 3300e	-	All	All	All
Hardware	Fortinet	Fortigate 3600e	-	All	All	All
Hardware	Fortinet	Fortigate 40f	-	All	All	All
Hardware	Fortinet	Fortigate 60f	-	All	All	All
Hardware	Fortinet	Fortigate 7121f	-	All	All	All
Operating System	Fortinet	Fortios	7.0.0	All	All	All
Operating System	Fortinet	Fortios	7.0.1	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

References

Reference	Source	Link	Tags
PSIRT Advisories | FortiGuard	CONFIRM	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

43912 FortiOS Heap-based Buffer Overflow Vulnerability (FG-IR-21-115)