



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)						

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)