



CVE-2016-8492

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

Summary

CVE	CVE-2016-8492
State	PUBLIC
Assigner	psirt@fortinet.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-08 16:59:00 UTC
Updated	2017-03-02 16:18:00 UTC
Description	The implementation of an ANSI X9.31 RNG in Fortinet FortiGate allows attackers to gain unauthorized read access to data

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fortinet	Fortios	4.3.0	All	All	All
Operating System	Fortinet	Fortios	4.3.10	All	All	All
Operating System	Fortinet	Fortios	4.3.12	All	All	All
Operating System	Fortinet	Fortios	4.3.13	All	All	All
Operating System	Fortinet	Fortios	4.3.14	All	All	All
Operating System	Fortinet	Fortios	4.3.15	All	All	All
Operating System	Fortinet	Fortios	4.3.16	All	All	All
Operating System	Fortinet	Fortios	4.3.17	All	All	All
Operating System	Fortinet	Fortios	4.3.0	All	All	All
Operating System	Fortinet	Fortios	4.3.10	All	All	All
Operating System	Fortinet	Fortios	4.3.12	All	All	All
Operating System	Fortinet	Fortios	4.3.13	All	All	All
Operating System	Fortinet	Fortios	4.3.14	All	All	All
Operating System	Fortinet	Fortios	4.3.15	All	All	All
Operating System	Fortinet	Fortios	4.3.16	All	All	All
Operating System	Fortinet	Fortios	4.3.17	All	All	All
Operating System	Fortinet	Fortios	All	All	All	All

References			
Reference	Source	Link	Tags
DUHK Attack against Fortinet Products FortiGuard	CONFIRM	fortiguard.com	Vendor Advisory
Fortinet FortiOS CVE-2016-8492 Information Disclosure Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Entr
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.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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