



CVE-2015-5698

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2015-5698
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-30 14:59:00 UTC
Updated	2023-05-15 17:15:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the web server on Siemens SIMATIC S7-1200 CPU devices with firmware

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Simatic S7 1200 Cpu	-	All	All	All
Hardware	Siemens	Simatic S7 1200 Cpu	-	All	All	All
Operating System	Siemens	Simatic S7 1200 Cpu Firmware	All	All	All	All

References

Reference	Source
Siemens SIMATIC S7-1200 CSRF Vulnerability ICS-CERT	MISC
Siemens SIMATIC S7-1200 Cross Site Request Forgery ~ Packet Storm	MISC
Siemens SIMATIC S7-1200 Access Control Flaw Lets Remote Users Conduct Cross-Site Request Forgery Attacks - SecurityTracker	SECT
Siemens	CONF
cert-portal.siemens.com/productcert/pdf/ssa-134003.pdf	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#)