CVE-2016-3949

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

Summary

CVE	CVE-2016-3949
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-27 10:59:00 UTC
Updated	2020-02-10 15:15:00 UTC
Description	Siemens SIMATIC S7-300 Profinet-enabled CPU devices with firmware before 3.2.12 and SIMATIC S7-300 Profinet-disable

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Simatic S7-300 Without Profitnet Support	All	All	All	All
Hardware	Siemens	Simatic S7-300 Without Profitnet Support	All	All	All	All
Operating System	Siemens	Simatic S7-300 Without Profitnet Support Firmware	3.3.11	All	All	All
Operating System	Siemens	Simatic S7-300 Without Profitnet Support Firmware	3.3.11	All	All	All
Hardware	Siemens	Simatic S7-300 With Profitnet Support	All	All	All	All
Hardware	Siemens	Simatic S7-300 With Profitnet Support	All	All	All	All
Operating System	Siemens	Simatic S7-300 With Profitnet Support Firmware	3.2.11	All	All	All
Operating System	Siemens	Simatic S7-300 With Profitnet Support Firmware	3.2.11	All	All	All

References

Reference	Source
cert-portal.siemens.com/productcert/pdf/ssa-818183.pdf	CONFIRM
Siemens SIMATIC S7-300 Denial-of-Service Vulnerability | ICS-CERT	MISC
Siemens SIMATIC S7-300 CPU TSAP Processing Flaw Lets Remote Users Cause the Target System to Crash - SecurityTracker	SECTRAC
Siemens	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

591197 Siemens SIMATIC S7-300 Denial of Service (DoS) Vulnerability (ICSA-16-161-01, SSA-818183)