CVE-2016-20009

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

Summary

CVE	CVE-2016-20009
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-11 22:15:00 UTC
Updated	2023-11-07 02:30:00 UTC
Description	** UNSUPPORTED WHEN ASSIGNED ** A DNS client stack-based buffer overflow in ipdnsc_decode_name() affects Winc

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Sgt-100	-	All	All	All
Operating System	Siemens	Sgt-100 Firmware	All	All	All	All
Hardware	Siemens	Sgt-200	-	All	All	All
Operating System	Siemens	Sgt-200 Firmware	All	All	All	All
Hardware	Siemens	Sgt-300	-	All	All	All
Operating System	Siemens	Sgt-300 Firmware	All	All	All	All
Hardware	Siemens	Sgt-400	-	All	All	All
Operating System	Siemens	Sgt-400 Firmware	All	All	All	All
Hardware	Siemens	Sgt-a20	-	All	All	All
Operating System	Siemens	Sgt-a20 Firmware	All	All	All	All
Hardware	Siemens	Sgt-a35	-	All	All	All
Operating System	Siemens	Sgt-a35 Firmware	All	All	All	All
Hardware	Siemens	Sgt-a65	-	All	All	All
Operating System	Siemens	Sgt-a65 Firmware	All	All	All	All
Operating System	Windriver	Vxworks	All	All	All	All

References

Reference	Source	Link	Tags
VxWorks: Execute My Packets | Exodus Intelligence	MISC	blog.exodusintel.com	Exploit, Third Party Advisory
cert-portal.siemens.com/productcert/pdf/ssa-553445.pdf	CONFIRM	cert-portal.siemens.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

590759 Siemens Energy AGT and SGT Solutions Vulnerability (ICSA-21-222-06)

591039 Rockwell Automation Multiple Products Domain Name System (DNS) Remote Code Execution (RCE) Vulnerability (PN1564)

730368 Wind River VxWorks Out-of-bounds Write Vulnerability