CVE-2021-41990

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-41990
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-18 14:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	The gmp plugin in strongSwan before 5.9.4 has a remote integer overflow via a crafted certificate with an RSASSA-PSS sig

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Hardware	Siemens	6gk5615-0aa00-2aa2	-	All	All	All
Operating System	Siemens	6gk5615-0aa00-2aa2 Firmware	-	All	All	All
Hardware	Siemens	6gk5804-0ap00-2aa2	-	All	All	All
Operating System	Siemens	6gk5804-0ap00-2aa2 Firmware	-	All	All	All
Hardware	Siemens	6gk5812-1aa00-2aa2	-	All	All	All
Operating System	Siemens	6gk5812-1aa00-2aa2 Firmware	-	All	All	All
Hardware	Siemens	6gk5812-1ba00-2aa2	-	All	All	All
Operating System	Siemens	6gk5812-1ba00-2aa2 Firmware	-	All	All	All
Hardware	Siemens	6gk5816-1aa00-2aa2	-	All	All	All
Operating System	Siemens	6gk5816-1aa00-2aa2 Firmware	-	All	All	All
Hardware	Siemens	6gk5816-1ba00-2aa2	-	All	All	All
Operating System	Siemens	6gk5816-1ba00-2aa2 Firmware	-	All	All	All

Hardware	Siemens	6gk5826-2ab00-2ab2	-	All	All	All
Operating System	Siemens	6gk5826-2ab00-2ab2 Firmware	-	All	All	All
Hardware	Siemens	6gk5856-2ea00-3aa1	-	All	All	All
Operating System	Siemens	6gk5856-2ea00-3aa1 Firmware	-	All	All	All
Hardware	Siemens	6gk5856-2ea00-3da1	-	All	All	All
Operating System	Siemens	6gk5856-2ea00-3da1 Firmware	-	All	All	All
Hardware	Siemens	6gk5874-2aa00-2aa2	-	All	All	All
Operating System	Siemens	6gk5874-2aa00-2aa2 Firmware	-	All	All	All
Hardware	Siemens	6gk5874-3aa00-2aa2	-	All	All	All
Operating System	Siemens	6gk5874-3aa00-2aa2 Firmware	-	All	All	All
Hardware	Siemens	6gk5876-3aa02-2ba2	-	All	All	All
Operating System	Siemens	6gk5876-3aa02-2ba2 Firmware	-	All	All	All
Hardware	Siemens	6gk5876-3aa02-2ea2	-	All	All	All
Operating System	Siemens	6gk5876-3aa02-2ea2 Firmware	-	All	All	All
Hardware	Siemens	6gk5876-4aa00-2ba2	-	All	All	All
Operating System	Siemens	6gk5876-4aa00-2ba2 Firmware	-	All	All	All
Hardware	Siemens	6gk5876-4aa00-2da2	-	All	All	All
Operating System	Siemens	6gk5876-4aa00-2da2 Firmware	-	All	All	All
Hardware	Siemens	6gk6108-4am00-2ba2	-	All	All	All
Operating System	Siemens	6gk6108-4am00-2ba2 Firmware	-	All	All	All
Hardware	Siemens	6gk6108-4am00-2da2	-	All	All	All
Operating System	Siemens	6gk6108-4am00-2da2 Firmware	-	All	All	All
Application	Strongswan	Strongswan	All	All	All	All

References

Reference	Source	Link
Release strongSwan 5.9.4 · strongswan/strongswan · GitHub	MISC	github.com
Debian -- Security Information -- DSA-4989-1 strongswan	DEBIAN	www.debian.org
strongSwan - strongSwan Vulnerability (CVE-2021-41990)		www.strongswan.org
[SECURITY] Fedora 35 Update: strongswan-5.9.4-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
strongSwan - strongSwan Vulnerability (CVE-2021-41990)	CONFIRM	www.strongswan.org
[SECURITY] Fedora 35 Update: strongswan-5.9.4-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: strongswan-5.9.4-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 33 Update: strongswan-5.9.4-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
cert-portal.siemens.com/productcert/pdf/ssa-539476.pdf	CONFIRM	cert-portal.siemens.com

[SECURITY] Fedora 33 Update: strongswan-5.9.4-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 34 Update: strongswan-5.9.4-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 178824 Debian Security Update for strongswan (DSA 4989-1)
- 183320 Debian Security Update for strongswan (CVE-2021-41990)
- 198539 Ubuntu Security Notification for strongSwan Vulnerabilities (USN-5111-1)
- 282015 Fedora Security Update for strongswan (FEDORA-2021-0b37146973)
- 282016 Fedora Security Update for strongswan (FEDORA-2021-b3df83339e)
- 500669 Alpine Linux Security Update for strongswan
- 501500 Alpine Linux Security Update for strongswan
- 501785 Alpine Linux Security Update for strongswan
- 502034 Alpine Linux Security Update for strongswan
- 504439 Alpine Linux Security Update for strongswan
- 610398 Google Android February 2022 Security Patch Missing for Samsung
- 690851 Free Berkeley Software Distribution (FreeBSD) Security Update for strongswan (58528a94-5100-4208-a04d-edc01598cf01)
- 751255 SUSE Enterprise Linux Security Update for strongswan (SUSE-SU-2021:3469-1)
- 751259 OpenSUSE Security Update for strongswan (openSUSE-SU-2021:3467-1)
- 751299 OpenSUSE Security Update for strongswan (openSUSE-SU-2021:1399-1)
- 900401 Common Base Linux Mariner (CBL-Mariner) Security Update for strongswan (6025)
- 901614 Common Base Linux Mariner (CBL-Mariner) Security Update for strongswan (6896-1)

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