CVE-2023-0361

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-0361
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-15 18:15:00 UTC
Updated	2023-11-07 04:00:00 UTC
Description	A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel

Risk And Classification

Problem Types: CWE-203

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	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Gnu	Gnutls	3.6.8-11.el8_2	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Converged Systems Advisor Agent	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 36 Update: gnutls-3.8.0-2.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Timing sidechannel in RSA decryption (#1050) · Issues · gnutls / GnuTLS · GitLab	MISC	gitlab.com
[SECURITY] Fedora 37 Update: gnutls-3.8.0-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
July 2023 MySQL Server Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com

[SECURITY] Fedora 38 Update: guile-gnutls-3.7.11-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 37 Update: gnutls-3.8.0-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE-2023-0361 GNU TLS Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 36 Update: gnutls-3.8.0-2.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 3321-1] gnutls28 security update	MLIST	lists.debian.org
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com
Timing attacks - docs and minor fixes by tomato42 · Pull Request #679 · tlsfuzzer/tlsfuzzer · GitHub	MISC	github.com
[SECURITY] Fedora 38 Update: guile-gnutls-3.7.11-1.fc38 - 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

160497 Oracle Enterprise Linux Security Update for gnutls (ELSA-2023-1141)

160526 Oracle Enterprise Linux Security Update for gnutls (ELSA-2023-1569)

181559 Debian Security Update for gnutls28 (DSA 5349-1)

181582 Debian Security Update for gnutls28 (DLA 3321-1)

181897 Debian Security Update for gnutls28 (CVE-2023-0361)

199200 Ubuntu Security Notification for GnuTLS Vulnerability (USN-5901-1)

241240 Red Hat Update for gnutls (RHSA-2023:1141)

241255 Red Hat Update for gnutls (RHSA-2023:1200)

241322 Red Hat Update for gnutls (RHSA-2023:1569)

241563 Red Hat Update for gnutls (RHSA-2023:3361)

283752 Fedora Security Update for gnutls (FEDORA-2023-1c4a6a47ae)

283805 Fedora Security Update for gnutls (FEDORA-2023-4fc4c33f2b)

284274 Fedora Security Update for gnutls (FEDORA-2023-5b378b82b3)

355188 Amazon Linux Security Advisory for gnutls : ALAS2023-2023-171

378414 Alibaba Cloud Linux Security Update for gnutls (ALINUX3-SA-2023:0035)

502659 Alpine Linux Security Update for gnutls

502660 Alpine Linux Security Update for gnutls

502729 Alpine Linux Security Update for gnutls

503109 Alpine Linux Security Update for gnutls

505875 Alpine Linux Security Update for gnutls

672986 EulerOS Security Update for gnutls (EulerOS-SA-2023-1843)

672991 EulerOS Security Update for gnutls (EulerOS-SA-2023-1868)

673025 EulerOS Security Update for gnutls (EulerOS-SA-2023-1953)

673051 EulerOS Security Update for gnutls (EulerOS-SA-2023-1975)

673138 EulerOS Security Update for gnutls (EulerOS-SA-2023-2291)

673155 EulerOS Security Update for gnutls (EulerOS-SA-2023-2267)

691059 Free Berkeley Software Distribution (FreeBSD) Security Update for gnutls (0a7a5dfb-aba4-11ed-be2c-001cc0382b2f)

691232 Free Berkeley Software Distribution (FreeBSD) Security Update for mysql (759a5599-3ce8-11ee-a0d1-84a93843eb75)

753740 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2023:0610-1)

755523 SUSE Enterprise Linux Security Update for gnutls (SUSE-SU-2023:4952-1)

905557 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (13574)

905565 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (13568)

906543 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (13574-1)

906601 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (13574-3)

906689 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (13568-3)

906775 Common Base Linux Mariner (CBL-Mariner) Security Update for gnutls (13574-5)

940958 AlmaLinux Security Update for gnutls (ALSA-2023:1141)

940969 AlmaLinux Security Update for gnutls (ALSA-2023:1569)

960668 Rocky Linux Security Update for gnutls (RLSA-2023:1141)

960894 Rocky Linux Security Update for gnutls (RLSA-2023:1569)