CVE-2021-3580

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3580
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-05 21:15:00 UTC
Updated	2024-01-16 15:15:00 UTC
Description	A flaw was found in the way nettle's RSA decryption functions handled specially crafted ciphertext. An attacker could use th

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Nettle Project	Nettle	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
CVE-2021-3580 Nettle Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.neta
[SECURITY] [DLA 2760-1] nettle security update	MLIST	lists.debian.c
1967983 – (CVE-2021-3580) CVE-2021-3580 nettle: Remote crash in RSA decryption via manipulated ciphertext	MISC	bugzilla.redh
Nettle: Denial of Service (GLSA 202401-24) — Gentoo security		security.gent
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

159515 Oracle Enterprise Linux Security Update for gnutls and nettle (ELSA-2021-4451)

159717 Oracle Enterprise Linux Security Update for gnutls (ELSA-2022-9221)

178677 Debian Security Update for nettle (DSA 4933-1)

178806 Debian Security Update for nettle (DLA 2760-1)

179899 Debian Security Update for nettle (CVE-2021-3580)

198408 Ubuntu Security Notification for Nettle vulnerabilities (USN-4990-1)

239785 Red Hat Update for gnutls and nettle security (RHSA-2021:4451)

296065 Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)

500421 Alpine Linux Security Update for nettle

501442 Alpine Linux Security Update for nettle

504180 Alpine Linux Security Update for nettle

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

670653 EulerOS Security Update for nettle (EulerOS-SA-2021-2411)

670717 EulerOS Security Update for nettle (EulerOS-SA-2021-2475)

670754 EulerOS Security Update for nettle (EulerOS-SA-2021-2512)

670778 EulerOS Security Update for nettle (EulerOS-SA-2021-2536)

670802 EulerOS Security Update for nettle (EulerOS-SA-2021-2560)

671017 EulerOS Security Update for nettle (EulerOS-SA-2021-2598)

710842 Gentoo Linux Nettle Denial of Service (DoS) Vulnerability (GLSA 202401-24)

750700 SUSE Enterprise Linux Security Update for libnettle (SUSE-SU-2021:2135-1)

750701 SUSE Enterprise Linux Security Update for libnettle (SUSE-SU-2021:2143-1)

750717 OpenSUSE Security Update for libnettle (openSUSE-SU-2021:0906-1)

750784 OpenSUSE Security Update for libnettle (openSUSE-SU-2021:2143-1)

900295 CBL-Mariner Linux Security Update for nettle 3.7.2

901411 Common Base Linux Mariner (CBL-Mariner) Security Update for nettle (6741-1)

902893 Common Base Linux Mariner (CBL-Mariner) Security Update for nettle (5124)

940170 AlmaLinux Security Update for gnutls and nettle (ALSA-2021:4451)

960167 Rocky Linux Security Update for gnutls and nettle (RLSA-2021:4451)