CVE-2021-20305

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-20305
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-05 22:15:00 UTC
Updated	2023-11-07 03:29:00 UTC
Description	A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDS

Risk And Classification

Problem Types: CWE-787

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	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Netapp	Active Iq Unified Manager	-	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-2021-20305 Nettle Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.
Debian -- Security Information -- DSA-4933-1 nettle	DEBIAN	www.debian.org
[SECURITY] [DLA 2760-1] nettle security update	MLIST	lists.debian.org
[SECURITY] Fedora 33 Update: gnutls-3.6.16-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproje
[SECURITY] Fedora 33 Update: gnutls-3.6.16-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproje
1942533 – (CVE-2021-20305) CVE-2021-20305 nettle: Out of Bound memory access in signature verification	MISC	bugzilla.redhat.c

Nettle: Denial of service (GLSA 202105-31) — Gentoo security	GENTOO	security.gentoo.
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

159146 Oracle Enterprise Linux Security Update for nettle (ELSA-2021-1145)

159150 Oracle Enterprise Linux Security Update for gnutls and nettle (ELSA-2021-1206)

174949 SUSE Enterprise Linux Security Update for libnettle (SUSE-SU-2021:1399-1)

174959 SUSE Enterprise Linux Security Update for libnettle (SUSE-SU-2021:1412-1)

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

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

179505 Debian Security Update for nettle (CVE-2021-20305)

198322 Ubuntu Security Notification for Nettle vulnerability (USN-4906-1)

239215 Red Hat Update for nettle (RHSA-2021:1145)

239220 Red Hat Update for gnutls and nettle (RHSA-2021:1206)

239241 Red Hat Update for gnutls and nettle (RHSA-2021:1246)

239242 Red Hat Update for gnutls and nettle (RHSA-2021:1245)

239414 Red Hat Update for nettle (RHSA-2021:2280)

257076 CentOS Security Update for nettle (CESA-2021:1145)

281107 Fedora Security Update for gnutls (FEDORA-2021-454a0f6f76)

296059 Oracle Solaris 11.4 Support Repository Update (SRU) 36.0.1.101.2 Missing (CPUJUL2021)

352269 Amazon Linux Security Advisory for nettle: ALAS2-2021-1629

375673 F5 BIG-IP ASM,LTM,APM BIG-IP Nettle Cryptography Library Vulnerability (K33101555)

377030 Alibaba Cloud Linux Security Update for nettle (ALINUX2-SA-2021:0018)

377158 Alibaba Cloud Linux Security Update for gnutls and nettle (ALINUX3-SA-2021:0029)

501441 Alpine Linux Security Update for nettle

504179 Alpine Linux Security Update for nettle

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

670549 EulerOS Security Update for nettle (EulerOS-SA-2021-2307)

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

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

710083 Gentoo Linux Nettle Denial of service (GLSA 202105-31)

730121 McAfee Web Gateway Multiple Vulnerabilities (WP-3484,WP-3744,WP-3745,WP-3746,WP-3747,WP-3793,WP-3800)

750241 OpenSUSE Security Update for libnettle (openSUSE-SU-2021:0635-1)

900066 CBL-Mariner Linux Security Update for nettle 3.4.1

903108 Common Base Linux Mariner (CBL-Mariner) Security Update for nettle (4053)

940036 AlmaLinux Security Update for gnutls and nettle (ALSA-2021:1206)

960830 Rocky Linux Security Update for gnutls and nettle (RLSA-2021:1206)