CVE-2021-3716

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3716
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 23:15:00 UTC
Updated	2023-07-07 19:27:00 UTC
Description	A flaw was found in nbdkit due to to improperly caching plaintext state across the STARTTLS encryption boundary. A MitM

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nbdkit Project	Nbdkit	All	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
[Libguestfs] [NBDKIT SECURITY] STARTTLS denial-of-service weakness	MISC	listman.redh
server: CVE-2021-3716 reset structured replies on starttls (09a13daf) · Commits · nbdkit / nbdkit · GitLab	MISC	gitlab.com
oss-security - Re: STARTTLS vulnerabilities	MISC	www.openw
1994695 – (CVE-2021-3716) CVE-2021-3716 nbdkit: NBD_OPT_STRUCTURED_REPLY injection on STARTTLS	MISC	bugzilla.red
server: reset meta context replies on starttls (6c5faac6) · Commits · nbdkit / nbdkit · GitLab	MISC	gitlab.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159858 Oracle Enterprise Linux Security Update for virt:ol and virt-devel:ol (ELSA-2022-1759)

182726 Debian Security Update for nbdkit (CVE-2021-3716)

240292 Red Hat Update for virt:rhel and virt-devel:rhel security (RHSA-2022:1759)

281862 Fedora Security Update for nbdkit (FEDORA-2021-9c2ba2fcfc)

281863 Fedora Security Update for nbdkit (FEDORA-2021-535596f062)

901588 Common Base Linux Mariner (CBL-Mariner) Security Update for nbdkit (8873)

940525 AlmaLinux Security Update for virt:rhel and virt-devel:rhel (ALSA-2022:1759)

960314 Rocky Linux Security Update for virt:rhel and virt-devel:rhel (RLSA-2022:1759)