CVE-2020-10769

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-10769
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-26 16:15:00 UTC
Updated	2023-02-12 23:39:00 UTC
Description	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference
Red Hat Customer Portal - Access to 24x7 support and knowledge
LKML: Greg Kroah-Hartman: [PATCH 4.14 21/59] crypto: authenc - fix parsing key with misaligned rta_len
Red Hat Customer Portal
1708775 – (CVE-2020-10769) CVE-2020-10769 kernel: Buffer over-read in crypto_authenc_extractkeys() when a payload longer than 4 bytes
Red Hat Customer Portal - Access to 24x7 support and knowledge
1708775 – (CVE-2020-10769) CVE-2020-10769 kernel: Buffer over-read in crypto_authenc_extractkeys() when a payload longer than 4 bytes
Red Hat Customer Portal - Access to 24x7 support and knowledge
[security-announce] openSUSE-SU-2020:1153-1: important: Security update
1708775 – (CVE-2020-10769) CVE-2020-10769 kernel: Buffer over-read in crypto_authenc_extractkeys() when a payload longer than 4 bytes
Oracle Critical Patch Update Advisory - April 2021

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

174728 SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2020:2122-1)

174729 SUSE Enterprise Linux Security update for the Linux Kernel (SUSE-SU-2020:2106-1)

752231 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2082-1)