CVE-2021-3565

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-3565
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-04 12:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	A flaw was found in tpm2-tools in versions before 5.1.1 and before 4.3.2. tpm2_import used a fixed AES key for the inner w

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Tpm2-tools Project	Tpm2-tools	All	All	All	All

References

Reference	Source	Link	Ta
[SECURITY] Fedora 34 Update: tpm2-tools-5.1.1-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
1964427 – (CVE-2021-3565) CVE-2021-3565 tpm2-tools: fixed AES wrapping key in tpm2_import	MISC	bugzilla.redhat.com	
[SECURITY] Fedora 33 Update: tpm2-tools-4.3.2-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: tpm2-tools-4.3.2-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: tpm2-tools-5.1.1-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159511	Oracle Enterprise Linux Security Update for tpm2-tools (ELSA-2021-4413)
179835	Debian Security Update for tpm2-tools (CVE-2021-3565)
239880	Red Hat Update for tpm2-tools (RHSA-2021:4413)
281666	Fedora Security Update for tpm2 (FEDORA-2021-00a15ad850)
281667	Fedora Security Update for tpm2 (FEDORA-2021-c970c02748)
750661	SUSE Enterprise Linux Security Update for tpm2.0-tools (SUSE-SU-2021:1999-1)
750664	SUSE Enterprise Linux Security Update for tpm2.0-tools (SUSE-SU-2021:1998-1)
750723	OpenSUSE Security Update for tpm2.0-tools (openSUSE-SU-2021:0934-1)
750767	OpenSUSE Security Update for tpm2.0-tools (openSUSE-SU-2021:1998-1)
900222	CBL-Mariner Linux Security Update for tpm2-tools 4.2
900962	Common Base Linux Mariner (CBL-Mariner) Security Update for tpm2-tools (6923-1)
903639	Common Base Linux Mariner (CBL-Mariner) Security Update for tpm2-tools (4345)
940129	AlmaLinux Security Update for tpm2-tools (ALSA-2021:4413)
960260	Rocky Linux Security Update for tpm2-tools (RLSA-2021:4413)