CVE-2017-7526

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-7526
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-26 13:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	libgcrypt before version 1.7.8 is vulnerable to a cache side-channel attack resulting into a complete break of RSA-1024 whil

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Gnupg	Libgcrypt	All	All	All	All
Application	Gnupg	Libgcrypt	All	All	All	All

References

Reference
Cryptology ePrint Archive: Report 2017/627
git.gnupg.org Git - libgcrypt.git/commit

git.gnupg.org Git - libgcrypt.git/commit
Debian -- Security Information -- DSA-3901-1 libgcrypt20
git.gnupg.org Git - libgcrypt.git/commit
USN-3733-1: GnuPG vulnerability | Ubuntu security notices
git.gnupg.org Git - libgcrypt.git/commit
USN-3733-2: GnuPG vulnerability | Ubuntu security notices
git.gnupg.org Git - libgcrypt.git/commit
1466265 – (CVE-2017-7526) CVE-2017-7526 libgcrypt: Use of left-to-right sliding window method allows full RSA key recovery
git.gnupg.org Git - libgcrypt.git/commit
[Announce] Libgcrypt 1.7.8 released to fix CVE-2017-7526
Libgcrypt CVE-2017-7526 Information Disclosure Vulnerability
Debian -- Security Information -- DSA-3960-1 gnupg
Libgcrypt RSA-1024 Sliding-Window Expansion Side Channel Attack Lets Remote Users Recover Keys Used by the Target System in Certain
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500359 Alpine Linux Security Update for gnupg1
671105 EulerOS Security Update for libgcrypt (EulerOS-SA-2019-2205)