CVE-2014-5119

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

Summary

CVE	CVE-2014-5119
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-29 16:55:00 UTC
Updated	2023-02-13 00:42:00 UTC
Description	Off-by-one error in the __gconv_translit_find function in gconv_trans.c in GNU C Library (aka glibc) allows context-depende

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Gnu	Glibc	All	All	All	All
Application	Gnu	Glibc	All	All	All	All

References

Reference
1119128 – (CVE-2014-5119) CVE-2014-5119 glibc: off-by-one error leading to a heap-based buffer overflow flaw in __gconv_translit_find()
Security Advisory SA60358 - Red Hat update for glibc - Secunia
Red Hat Customer Portal
Red Hat Customer Portal
GNU glibc '__gconv_translit_find()' Function Local Heap Based Buffer Overflow Vulnerability
access.redhat.com | CVE-2014-5119
Cisco Unified Communications Manager glibc Arbitrary Code Execution Vulnerability
Bug 17187 – Out-of-bounds NUL write in iconv_open (CVE-2014-5119)
About Secunia Research | Flexera
[security-announce] SUSE-SU-2014:1125-1: important: Security update for

RETIRED: Cisco Unified Communications Manager Local Heap Based Buffer Overflow Vulnerability
Support / Security / Advisories / / MDVSA-2014:175 | Mandriva
oss-security - Re: [CVE Request] glibc iconv_open buffer overflow (was: Re: Re: glibc locale issues)
About Secunia Research | Flexera
Red Hat Customer Portal
GNU C Library: Multiple vulnerabilities (GLSA 201602-02) — Gentoo Security
oss-security - glibc locale issues
IBM Security Bulletin: Vulnerabilities in Bash and GNU C Library affect WebSphere Transformation Extender (WTX) with Launcher Hypervisor
Red Hat Customer Portal
About Secunia Research | Flexera
Debian -- Security Information -- DSA-3012-1 eglibc
Security Advisory SA61074 - Cisco Unified Communications Manager GNU C Library "__gconv_translit_find()" Off-By-One Vulnera
Issue 96 - google-security-research - glibc off-by-one NUL byte heap overflow in gconv_translit_find - Google Security Research - Google Proj
Project Zero: The poisoned NUL byte, 2014 edition
Full Disclosure: CVE-2014-5119 glibc __gconv_translit_find() exploit
linux.oracle.com | ELSA-2015-0092 - glibc security update
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**