CVE-2016-5419

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

Summary

CVE	CVE-2016-5419
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-10 14:59:00 UTC
Updated	2023-11-07 02:33:00 UTC
Description	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Haxx	Libcurl	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All

References

Reference
curl - TLS session resumption client cert bypass
openSUSE-SU-2016:2379-1: moderate: Security update for curl
[SECURITY] Fedora 24 Update: curl-7.47.1-6.fc24 - package-announce - Fedora Mailing-Lists
cURL/libcurl TLS Session Resumption Client Certificate Bug Lets Remote Users Bypass Security Restrictions on the Target System - Security
Red Hat Customer Portal
Red Hat Customer Portal
openSUSE-SU-2016:2227-1: moderate: Security update for curl
[R7] LCE 4.8.1 Fixes Multiple Vulnerabilities - Security Advisory | Tenable™
cURL/libcurl TLS Session Resumption Client Certificate Bug Lets Remote Users Bypass Security Restrictions on the Target System - Security

[SECURITY] Fedora 23 Update: curl-7.43.0-8.fc23 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 23 Update: curl-7.43.0-8.fc23 - package-announce - Fedora Mailing-Lists
cURL/libcURL CVE-2016-5419 Information Disclosure Vulnerability
cURL/libcURL CVE-2016-5419 Remote Security Bypass Vulnerability
[SECURITY] Fedora 24 Update: curl-7.47.1-6.fc24 - package-announce - Fedora Mailing-Lists
Android Security Bulletin—December 2016 | Android Open Source Project
CPU Oct 2018
cURL: Multiple vulnerabilities (GLSA 201701-47) — Gentoo security
The Slackware Linux Project: Slackware Security Advisories
USN-3048-1: curl vulnerabilities | Ubuntu
Debian -- Security Information -- DSA-3638-1 curl
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500111	Alpine Linux Security Update for curl
503766	Alpine Linux Security Update for curl
710385	Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201701-47)