CVE-2016-7141

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

Summary

CVE	CVE-2016-7141
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-03 21:59:00 UTC
Updated	2018-11-13 11:29:00 UTC
Description	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attacke

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	Source
openSUSE-SU-2016:2379-1: moderate: Security update for curl	SUSE
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Bug 1373229 – CVE-2016-7141 curl: Incorrect reuse of client certificates	CONFIRM
cURL/libcurl Certificate Reuse Bug Lets Remote Users Bypass Security Restrictions on the Target System - SecurityTracker	SECTRACK
[SECURITY] [DLA 1568-1] curl security update	MLIST
nss: refuse previously loaded certificate from file · curl/curl@7700fcb · GitHub	CONFIRM
CPU Oct 2018	CONFIRM
cURL/libcURL CVE-2016-7141 Certificate Validation Security Bypass Vulnerability	BID
curl - Incorrect reuse of client certificates	CONFIRM
cURL: Multiple vulnerabilities (GLSA 201701-47) — Gentoo security	GENTOO

Red Hat Customer Portal	REDHAT
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500112 Alpine Linux Security Update for curl

503767 Alpine Linux Security Update for curl

710385 Gentoo Linux cURL Multiple Vulnerabilities (GLSA 201701-47)