CVE-2015-1263

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

Summary

CVE	CVE-2015-1263
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-20 10:59:00 UTC
Updated	2023-11-07 02:24:00 UTC
Description	The Spellcheck API implementation in Google Chrome before 43.0.2357.65 does not use an HTTPS session for downloadi

Risk And Classification

Problem Types: CWE-17

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	Google	Chrome	All	All	All	All

References

Reference
Chromium: Multiple vulnerabilities (GLSA 201506-04) — Gentoo security
Debian -- Security Information -- DSA-3267-1 chromium-browser
Chrome Releases: Stable Channel Update
Issue 1056103005: [Spellcheck] Switch to https download - Code Review
openSUSE-SU-2015:1877-1: moderate: Security update for Chromium
Object not found!
Google Chrome Prior to 43.0.2357.65 Multiple Security Vulnerabilities
Google Chrome Multiple Bugs Let Remote Users Execute Arbitrary Code, Bypass Same-Origin Restrictions, and Spoof URLs - SecurityTracke
Issue 479162 - chromium - Security: spell checking dictionaries are fetched over HTTP, and large responses lead to a crash - Monorail
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**