



CVE-2017-5121

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-5121
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-27 05:29:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	Inappropriate use of JIT optimisation in V8 in Google Chrome prior to 61.0.3163.100 for Linux, Windows, and Mac allowed :

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

References

Reference	Source
Browser security beyond sandboxing – Windows Security blog	MISC
Google Chrome Out-of-Bounds Access Errors Let Remote Users Execute Arbitrary Code on the Target System - SecurityTracker	SECTRA
Google Chrome V8 Multiple Out-of-Bounds Memory Access Vulnerabilities	BID
Debian -- Security Information -- DSA-3985-1 chromium-browser	DEBIAN
Sign in - Google Accounts	
Chromium: Multiple vulnerabilities (GLSA 201709-25) — Gentoo Security	
Red Hat Customer Portal	REDHAT
Chrome Releases: Stable Channel Update for Desktop	
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
No vendor comments have been submitted for this CVE.	
Legacy QID Mappings	
710466 Gentoo Linux Chromium Multiple Vulnerabilities (GLSA 201709-25)	