CVE-2022-28109

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

Summary

CVE	CVE-2022-28109
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-15 16:15:00 UTC
Updated	2022-04-25 16:24:00 UTC
Description	Selenium Selenium Grid (formerly Selenium Standalone Server) Fixed in 4.0.0-alpha-7 is affected by: DNS rebinding. The i

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Selenium	Selenium Grid	All	All	All	All
Application	Selenium	Selenium Grid	4.0.0	-	All	All
Application	Selenium	Selenium Grid	4.0.0	alpha1	All	All
Application	Selenium	Selenium Grid	4.0.0	alpha2	All	All
Application	Selenium	Selenium Grid	4.0.0	alpha3	All	All
Application	Selenium	Selenium Grid	4.0.0	alpha4	All	All
Application	Selenium	Selenium Grid	4.0.0	alpha5	All	All
Application	Selenium	Selenium Grid	4.0.0	alpha6	All	All

References

Reference	Source	Link	Tags
CSRF and DNS-rebinding to RCE in Selenium Server (Grid) - /dev/posts/	MISC	www.gabriel.urdhr.fr	
oss-security - Re: Browser-mediated attacks on WebDriver servers	MLIST	www.openwall.com	
oss-security - Browser-mediated attacks on WebDriver servers	MISC	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730603 Selenium Server (Grid) Domain Name System (DNS) Rebinding Remote Code Execution (RCE) Vulnerability (GHSA-r2fp-xp6r-99gj)