



CVE-2020-35459

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

Summary

CVE	CVE-2020-35459
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-12 15:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	An issue was discovered in ClusterLabs crmsh through 4.2.1. Local attackers able to call "crm history" (when "crm" is run) v

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clusterlabs	Crmsh	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference	Source	Link
oss-security - Security issues in hawk2 and crmsh	CONFIRM	www.openwall.com
Releases · ClusterLabs/crmsh · GitHub	MISC	github.com
oss-security - Security issues in hawk2 and crmsh	MLIST	www.openwall.com
Bug 1179999 – VUL-0: CVE-2020-35459: crmsh: Root privilege escalation via hawk_invoke and crmsh	MISC	bugzilla.suse.com
[SECURITY] [DLA 2533-1] crmsh security update	MLIST	lists.debian.org
crmsh/history.py at a403aa15f3ea575adfe5e43bf2a31c9f9094fcda · ClusterLabs/crmsh · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

200227 Ubuntu Security Notification for CRM shell Vulnerability (USN-6711-1)

750296 OpenSUSE Security Update for hawk2 (openSUSE-SU-2021:0473-1)

750318 OpenSUSE Security Update for crmsh (openSUSE-SU-2021:0410-1)

750423 OpenSUSE Security Update for crmsh (openSUSE-SU-2021:0073-1)

750437 OpenSUSE Security Update for crmsh (openSUSE-SU-2021:0055-1)

750878 OpenSUSE Security Update for crmsh (openSUSE-SU-2021:2435-1)

750890 OpenSUSE Security Update for crmsh (openSUSE-SU-2021:1087-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)