



CVE-2020-10809

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

Summary

CVE	CVE-2020-10809
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-22 18:15:00 UTC
Updated	2020-04-30 13:22:00 UTC
Description	An issue was discovered in HDF5 through 1.12.0. A heap-based buffer overflow exists in the function Decompress() located

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hdfgroup	Hdf5	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2020-10809: Heap overflow in decompress.c – HDF5 - 1.13.0 - Loginsoft Research	MISC	research.loginsoft.com	Exploit, Thir
hdf5-reports/Vuln_1 at master · Loginsoft-Research/hdf5-reports · GitHub	MISC	github.com	Exploit, Thir
Source of RELEASE.txt - hdf5 - Bitbucket	MISC	bitbucket.hdfgroup.org	Release No
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[753223](#) SUSE Enterprise Linux Security Update for hdf5 (SUSE-SU-2022:1912-1)

[753231](#) SUSE Enterprise Linux Security Update for hdf5 (SUSE-SU-2022:1910-1)

[753383](#) SUSE Enterprise Linux Security Update for hdf5 (SUSE-SU-2022:1903-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

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