



# CVE-2022-48064

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2022-48064   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2023-08-22 19:16:00 UTC  |
| <b>Updated</b>         | 2023-11-07 03:56:00 UTC  |
| <b>Description</b>     | GNU Binutils before 2.40 was discovered to contain an excessive memory consumption vulnerability via the function bfd_dw |

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product  | Version | Update | Edition | Language |
|------------------|-------------------------------|--|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>                                     | 37      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>                                     | 38      | All    | All     | All      |
| Application      | <a href="#">Gnu</a>           | <a href="#">Binutils</a>                                   | All     | All    | All     | All      |
| Application      | <a href="#">Netapp</a>        | <a href="#">Ontap Select Deploy Administration Utility</a> | -       | All    | All     | All      |

## References

| Reference   | Source  | Link                                    | Tags |
|---|---------|---|------|
| 29922 – Huge memoy allocation in nm   | MISC    | <a href="#">sourceware.org</a>          |      |
| August 2023 GNU Binutils Vulnerabilities in NetApp Products   NetApp Product Security   | CONFIRM | <a href="#">security.netapp.com</a>     |      |
| [SECURITY] Fedora 37 Update: gdb-13.2-3.fc37 - package-announce - Fedora Mailing-Lists  |         | <a href="#">lists.fedoraproject.org</a> |      |
| [SECURITY] Fedora 39 Update: gdb-13.2-10.fc39 - package-announce - Fedora Mailing-Lists |         | <a href="#">lists.fedoraproject.org</a> |      |
| sourceware.org Git - binutils-gdb.git/commit  | MISC    | <a href="#">sourceware.org</a>          |      |
| [SECURITY] Fedora 38 Update: gdb-13.2-5.fc38 - package-announce - Fedora Mailing-Lists  | FEDORA  | <a href="#">lists.fedoraproject.org</a> |      |
| sourceware.org Git - binutils-gdb.git/commit  |         | <a href="#">sourceware.org</a>          |      |
| [SECURITY] Fedora 39 Update: gdb-13.2-10.fc39 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="#">lists.fedoraproject.org</a> |      |
| [SECURITY] Fedora 37 Update: gdb-13.2-3.fc37 - package-announce - Fedora Mailing-Lists  | FEDORA  | <a href="#">lists.fedoraproject.org</a> |      |
| [SECURITY] Fedora 38 Update: gdb-13.2-5.fc38 - package-announce - Fedora Mailing-Lists  |         | <a href="#">lists.fedoraproject.org</a> |      |

|                          |         |  |         |
|--------------------------|---------|--|---------|
| CVE Program record       | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>   | canonic |
| NVD vulnerability detail | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a> | canonic |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

|   |
|---|
| <a href="#">284554</a> Fedora Security Update for gdb (FEDORA-2023-d94be55511)                  |
| <a href="#">284620</a> Fedora Security Update for gdb (FEDORA-2023-8d0913f986)                  |
| <a href="#">285197</a> Fedora Security Update for gdb (FEDORA-2023-89ade611ee)                  |
| <a href="#">673433</a> EulerOS Security Update for binutils (EulerOS-SA-2023-3001)              |
| <a href="#">673470</a> EulerOS Security Update for binutils (EulerOS-SA-2023-3200)              |
| <a href="#">673545</a> EulerOS Security Update for binutils (EulerOS-SA-2023-3292)              |
| <a href="#">673613</a> EulerOS Security Update for binutils (EulerOS-SA-2023-3024)              |
| <a href="#">673629</a> EulerOS Security Update for binutils (EulerOS-SA-2023-3165)              |
| <a href="#">673756</a> EulerOS Security Update for gdb (EulerOS-SA-2024-1266)                   |
| <a href="#">673799</a> EulerOS Security Update for binutils (EulerOS-SA-2024-1257)              |
| <a href="#">673842</a> EulerOS Security Update for binutils (EulerOS-SA-2023-3324)              |
| <a href="#">673875</a> EulerOS Security Update for binutils (EulerOS-SA-2024-1133)              |
| <a href="#">674074</a> EulerOS Security Update for gdb (EulerOS-SA-2024-1137)                   |
| <a href="#">754877</a> SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2023:3695-1) |
| <a href="#">754965</a> SUSE Enterprise Linux Security Update for binutils (SUSE-SU-2023:3825-1) |
| <a href="#">755976</a> SUSE Enterprise Linux Security Update for gdb (SUSE-SU-2024:0899-1)      |
| <a href="#">755977</a> SUSE Enterprise Linux Security Update for gdb (SUSE-SU-2024:0898-1)      |
| <a href="#">755978</a> SUSE Enterprise Linux Security Update for gdb (SUSE-SU-2024:0898-1)      |

© [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](#)