# Binutils: binutils: arbitrary code execution via malformed xcoff object file processing

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-6846 |
| **State** | PUBLISHED |
| **Assigner** | redhat |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-22 09:16:27 UTC |
| **Updated** | 2026-04-22 09:16:27 UTC |
| **Description** | A flaw was found in binutils. A heap-buffer-overflow vulnerability exists when processing a specially crafted XCOFF (Extenc |

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from secalert@redhat.com

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**Problem Types:** CWE-122 | CWE-122 Heap-based Buffer Overflow

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | secalert@redhat.com | Primary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |

### CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Red Hat | Red Hat Enterprise Linux 10 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 10 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 10 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 10 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 6 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 7 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 7 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 9 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 9 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 9 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 9 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 9 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Hardened Images | Not specified | Not specified |
| CNA | Red Hat | Red Hat OpenShift Container Platform 4 | Not specified | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| access.redhat.com/security/cve/CVE-2026-6846 | secalert@redhat.com | access.redhat.com | |
| bugzilla.redhat.com/show_bug.cgi | secalert@redhat.com | bugzilla.redhat.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Red Hat would like to thank Takao Sato for reporting this issue. (en)

## Additional Advisory Data

| Source | Time | Event |
|---|---|---|
| CNA | 2026-04-08T00:00:00.000Z | Reported to Red Hat. |
| CNA | 2026-04-08T00:00:00.000Z | Made public. |

Workarounds

**CNA:** Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

There are currently no legacy QID mappings associated with this CVE.

© 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 registred 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**