



Libxml2: unbounded relaxng include recursion leading to stack overflow

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-0989 |
| State | PUBLISHED |
| Assigner | redhat |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-01-15 15:15:52 UTC |
| Updated | 2026-04-09 18:16:43 UTC |

Description A flaw was identified in the RelaxNG parser of libxml2 related to how external schema inclusions are handled. The parser d

Risk And Classification

Primary CVSS: v3.1 3.7 LOW from secalert@redhat.com

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

Problem Types: CWE-674 | CWE-674 Uncontrolled Recursion

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------------|-----------|-------|----------|---|
| 3.1 | secalert@redhat.com | Secondary | 3.7 | LOW | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L |
| 3.1 | CNA | CVSS | 3.7 | LOW | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

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 6 | 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 9 | Not specified | Not specified |
| CNA | Red Hat | Red Hat Hardened Images | Not specified | Not specified |
| CNA | Red Hat | Red Hat JBoss Core Services | 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-2026-0989 | secalert@redhat.com | access.redhat.com | |
| gitlab.gnome.org/GNOME/libxml2/-/issues/998 | secalert@redhat.com | gitlab.gnome.org | |
| 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 lanbigking for reporting this issue. (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|----------------------|
| CNA | 2026-01-15T12:36:12.129Z | Reported to Red Hat. |
| CNA | 2026-01-15T00:00:00.000Z | Made public. |

Workarounds

CNA: To mitigate this issue, restrict applications using libxml2 from processing untrusted RelaxNG schema files. Implement strict input validation and sanitization for all RelaxNG schema inputs to prevent the parsing of maliciously crafted, deeply nested include directives.

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 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](#)