



# XML::Parser versions through 2.47 for Perl has an off-by-one heap buffer overflow in st\_serial\_stack

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

## Summary

<b>CVE</b>	CVE-2006-10003
<b>State</b>	PUBLISHED
<b>Assigner</b>	CPANSec
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-19 12:16:17 UTC
<b>Updated</b>	2026-04-04 09:16:18 UTC
<b>Description</b>	XML::Parser versions through 2.47 for Perl has an off-by-one heap buffer overflow in st_serial_stack. In the case (stackptr -

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from nvd@nist.gov

[CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

**Problem Types:** CWE-122 | CWE-193 | CWE-193 CWE-193 Off-by-one Error | CWE-122  
CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</a>
3.1	ADP	DECLARED	9.8	CRITICAL	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</a>
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H</a>

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Toddr	Xml	\	parser	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TODDR	XMLParser	affected 2.47 custom	Not specified

### References

Reference	Source	Link
rt.cpan.org/Ticket/Display.html	9b29abf9-4ab0-4765-b253-1875cd9b441e	rt.cpan.org
github.com/cpan-authors/XML-Parser/issues/39	9b29abf9-4ab0-4765-b253-1875cd9b441e	github.com
github.com/cpan-authors/XML-Parser/commit/3eb9cc95420fa0c3f76947c4708962...	9b29abf9-4ab0-4765-b253-1875cd9b441e	github.com
www.openwall.com/lists/oss-security/2026/03/19/2	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
lists.debian.org/debian-lts-announce/2026/04/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

### Additional Advisory Data

Source	Time	Event
CNA	2006-06-13T00:00:00.000Z	Issue logged and patch provided in Request Tracker for XML::Parser
CNA	2019-09-23T00:00:00.000Z	Issue migrated to github issue tracker
CNA	2019-09-24T00:00:00.000Z	Patch provided in github issue tracker
CNA	2026-03-16T00:00:00.000Z	PR created and commit merged to git repo

### Solutions

**CNA:** Apply the patch that has been publicly available since 2006-06-13 or upgrade to version 2.48 or later when it is released.

## Workarounds

**CNA:** Apply the patch that has been publicly available since 2006-06-13.

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](#).

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