



# CVE-2012-1148

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

## Summary

<b>CVE</b>	CVE-2012-1148
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-07-03 19:55:00 UTC
<b>Updated</b>	2021-01-25 15:44:00 UTC
<b>Description</b>	Memory leak in the poolGrow function in expat/lib/xmlparse.c in expat before 2.1.0 allows context-dependent attackers to c

## Risk And Classification

**Problem Types:** CWE-399

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	All	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.1	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.2	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.4	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.5	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.6	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.7	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.8	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	2.0.0	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.1	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.2	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.4	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.5	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.6	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.7	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	1.95.8	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	2.0.0	All	All	All

Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	All	All	All	All
-------------	----------------------------------	--------------------------	-----	-----	-----	-----

## References

### Reference

[CVS Info for project expat](#)

[Expat XML Parser - Browse /expat/2.1.0 at SourceForge.net](#)

[Red Hat Customer Portal](#)

[USN-1613-2: Python 2.4 vulnerabilities | Ubuntu](#)

[APPLE-SA-2015-12-08-3 OS X El Capitan 10.11.2 and Security Update 2015-008](#)

[Debian -- Security Information -- DSA-2525-1 expat](#)

[Security Alerts - Secunia](#)

[Security Advisory SA51024 - Ubuntu update for python2.5 - Secunia](#)

[Expat XML Parsing Multiple Remote Denial of Service Vulnerabilities](#)

[Red Hat Customer Portal](#)

[Apple OS X Multiple Flaws Let Remote and Local Users Execute Arbitrary Code and Deny Service and Let Local Users Obtain Potentially Ser](#)

[About the security content of OS X El Capitan 10.11.2, Security Update 2015-005 Yosemite, and Security Update 2015-008 Mavericks - Apple](#)

[USN-1613-1: Python 2.5 vulnerabilities | Ubuntu](#)

[Expat XML Parser / Bugs / #485 memory leak in poolGrow](#)

[USN-1527-1: Expat vulnerabilities | Ubuntu](#)

[Support / Security / Advisories // MDVSA-2012:041 | Mandriva](#)

[Security Advisory SA51040 - Ubuntu update for python2.4 - Secunia](#)

[Red Hat Customer Portal](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

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](#)