



# CVE-2004-0594

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

## Summary

<b>CVE</b>	CVE-2004-0594
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-07-27 04:00:00 UTC
<b>Updated</b>	2018-10-30 16:25:00 UTC
<b>Description</b>	The memory_limit functionality in PHP 4.x up to 4.3.7, and 5.x up to 5.0.0RC3, under certain conditions such as when regis

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Avaya	Converged Communications Server	2.0	All	All	All
Hardware	Avaya	Converged Communications Server	2.0	All	All	All
Application	Avaya	Integrated Management	All	All	All	All
Application	Avaya	Integrated Management	All	All	All	All
Hardware	Avaya	S8300	r2.0.0	All	All	All
Hardware	Avaya	S8300	r2.0.1	All	All	All
Hardware	Avaya	S8300	r2.0.0	All	All	All
Hardware	Avaya	S8300	r2.0.1	All	All	All
Hardware	Avaya	S8500	r2.0.0	All	All	All
Hardware	Avaya	S8500	r2.0.1	All	All	All
Hardware	Avaya	S8500	r2.0.0	All	All	All
Hardware	Avaya	S8500	r2.0.1	All	All	All
Hardware	Avaya	S8700	r2.0.0	All	All	All
Hardware	Avaya	S8700	r2.0.1	All	All	All
Hardware	Avaya	S8700	r2.0.0	All	All	All
Hardware	Avaya	S8700	r2.0.1	All	All	All
Application	Php	Php	3.0	All	All	All

Application	Php	Php	3.0.1	All	All	All
Application	Php	Php	3.0.10	All	All	All
Application	Php	Php	3.0.11	All	All	All
Application	Php	Php	3.0.12	All	All	All
Application	Php	Php	3.0.13	All	All	All
Application	Php	Php	3.0.14	All	All	All
Application	Php	Php	3.0.15	All	All	All
Application	Php	Php	3.0.16	All	All	All
Application	Php	Php	3.0.17	All	All	All
Application	Php	Php	3.0.18	All	All	All
Application	Php	Php	3.0.2	All	All	All
Application	Php	Php	3.0.3	All	All	All
Application	Php	Php	3.0.4	All	All	All
Application	Php	Php	3.0.5	All	All	All
Application	Php	Php	3.0.6	All	All	All
Application	Php	Php	3.0.7	All	All	All
Application	Php	Php	3.0.8	All	All	All
Application	Php	Php	3.0.9	All	All	All
Application	Php	Php	4.0	All	All	All
Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.3	patch1	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All
Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All

Application	Php	Php	4.2	All	dev	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Application	Php	Php	3.0	All	All	All
Application	Php	Php	3.0.1	All	All	All
Application	Php	Php	3.0.10	All	All	All
Application	Php	Php	3.0.11	All	All	All
Application	Php	Php	3.0.12	All	All	All
Application	Php	Php	3.0.13	All	All	All
Application	Php	Php	3.0.14	All	All	All
Application	Php	Php	3.0.15	All	All	All
Application	Php	Php	3.0.16	All	All	All
Application	Php	Php	3.0.17	All	All	All
Application	Php	Php	3.0.18	All	All	All
Application	Php	Php	3.0.2	All	All	All
Application	Php	Php	3.0.3	All	All	All
Application	Php	Php	3.0.4	All	All	All
Application	Php	Php	3.0.5	All	All	All
Application	Php	Php	3.0.6	All	All	All
Application	Php	Php	3.0.7	All	All	All
Application	Php	Php	3.0.8	All	All	All
Application	Php	Php	3.0.9	All	All	All
Application	Php	Php	4.0	All	All	All

Application	Php	Php	4.0.1	All	All	All
Application	Php	Php	4.0.1	patch1	All	All
Application	Php	Php	4.0.1	patch2	All	All
Application	Php	Php	4.0.2	All	All	All
Application	Php	Php	4.0.3	All	All	All
Application	Php	Php	4.0.3	patch1	All	All
Application	Php	Php	4.0.4	All	All	All
Application	Php	Php	4.0.5	All	All	All
Application	Php	Php	4.0.6	All	All	All
Application	Php	Php	4.0.7	All	All	All
Application	Php	Php	4.0.7	rc1	All	All
Application	Php	Php	4.0.7	rc2	All	All
Application	Php	Php	4.0.7	rc3	All	All
Application	Php	Php	4.1.0	All	All	All
Application	Php	Php	4.1.1	All	All	All
Application	Php	Php	4.1.2	All	All	All
Application	Php	Php	4.2	All	dev	All
Application	Php	Php	4.2.0	All	All	All
Application	Php	Php	4.2.1	All	All	All
Application	Php	Php	4.2.2	All	All	All
Application	Php	Php	4.2.3	All	All	All
Application	Php	Php	4.3.0	All	All	All
Application	Php	Php	4.3.1	All	All	All
Application	Php	Php	4.3.2	All	All	All
Application	Php	Php	4.3.3	All	All	All
Application	Php	Php	4.3.5	All	All	All
Application	Php	Php	4.3.6	All	All	All
Application	Php	Php	4.3.7	All	All	All
Application	Php	Php	5.0	rc1	All	All
Application	Php	Php	5.0	rc2	All	All
Application	Php	Php	5.0	rc3	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_1.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Trustix	Secure Linux	1.5	All	All	All

Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	1.5	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.0	All	All	All
Operating System	<a href="#">Trustix</a>	<a href="#">Secure Linux</a>	2.1	All	All	All

## References

Reference	Source	Link
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Debian -- Security Information -- DSA-531-1 php4	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
'Advisory 11/2004: PHP memory_limit remote vulnerability' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>
[Full-Disclosure] Advisory 11/2004: PHP memory_limit remote vulnerability	FULLDISC	<a href="http://lists.grok.org.uk">lists.grok.org.uk</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibm.com">exchange.xforce.ibm.com</a>
'[security bulletin] SSRT4777 HP-UX Apache, PHP remote code execution, Denial of Service' - MARC	HP	<a href="http://marc.info">marc.info</a>
Home - Conectiva	CONNECTIVA	<a href="http://distro.conectiva.com">distro.conectiva.com</a>
'TSSA-2004-013 - php' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>
rhn.redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Debian -- Security Information -- DSA-669-1 php3	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
2004-0039	TRUSTIX	<a href="http://www.trustix.org">www.trustix.org</a>
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
PHP memory_limit Remote Code Execution Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
MandrakeSecure: MandrakeSoft Security Advisory MDKSA-2004:068 : php	MANDRAKE	<a href="http://www.mandrakesecurity.org">www.mandrakesecurity.org</a>
'[OpenPKG-SA-2004.034] OpenPKG Security Advisory (php)' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>
Gentoo Linux Documentation -- PHP: Multiple security vulnerabilities	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](#)**