



# CVE-2004-0488

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2004-0488
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-07-07 04:00:00 UTC
<b>Updated</b>	2023-11-07 01:56:00 UTC
<b>Description</b>	Stack-based buffer overflow in the ssl_util_uuencode_binary function in ssl_util.c for Apache mod_ssl, when mod_ssl is cor

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	Apache	Http Server	1.3	All	All	All
Application	Apache	Http Server	1.3.1	All	All	All
Application	Apache	Http Server	1.3.11	All	All	All
Application	Apache	Http Server	1.3.12	All	All	All
Application	Apache	Http Server	1.3.14	All	All	All
Application	Apache	Http Server	1.3.17	All	All	All
Application	Apache	Http Server	1.3.18	All	All	All
Application	Apache	Http Server	1.3.19	All	All	All
Application	Apache	Http Server	1.3.20	All	All	All
Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.24	All	All	All
Application	Apache	Http Server	1.3.25	All	All	All
Application	Apache	Http Server	1.3.26	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.28	All	All	All

Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.29	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.31	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.4	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.6	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.7	All	dev	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.9	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.28	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.28	beta	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.32	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.35	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.36	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.37	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.38	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.39	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.40	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.41	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.42	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.43	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.44	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.45	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.46	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.47	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.48	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.49	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0.9	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.11	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.12	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.14	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.17	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.18	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	1.3.19	All	All	All

Application	Apache	Http Server	1.3.20	All	All	All
Application	Apache	Http Server	1.3.22	All	All	All
Application	Apache	Http Server	1.3.23	All	All	All
Application	Apache	Http Server	1.3.24	All	All	All
Application	Apache	Http Server	1.3.25	All	All	All
Application	Apache	Http Server	1.3.26	All	All	All
Application	Apache	Http Server	1.3.27	All	All	All
Application	Apache	Http Server	1.3.28	All	All	All
Application	Apache	Http Server	1.3.29	All	All	All
Application	Apache	Http Server	1.3.3	All	All	All
Application	Apache	Http Server	1.3.31	All	All	All
Application	Apache	Http Server	1.3.4	All	All	All
Application	Apache	Http Server	1.3.6	All	All	All
Application	Apache	Http Server	1.3.7	All	dev	All
Application	Apache	Http Server	1.3.9	All	All	All
Application	Apache	Http Server	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Application	Apache	Http Server	2.0.9	All	All	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	1.4	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	amd64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.1	All	ppc	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.2	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.2	All	amd64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	10.0	All	amd64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.1	All	ppc	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.2	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	9.2	All	amd64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	2.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	2.1	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	2.1	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	2.1	All	x86_64	All
Application	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Multi Network Firewall</a>	8.2	All	All	All
Application	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Multi Network Firewall</a>	8.2	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.10	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.12	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.15	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.16	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.7	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.10	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.12	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.15	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.16	All	All	All
Application	<a href="#">Mod Ssl</a>	<a href="#">Mod Ssl</a>	2.8.7	All	All	All
Operating System	<a href="#">Openbsd</a>	<a href="#">Openbsd</a>	3.4	All	All	All
Operating System	<a href="#">Openbsd</a>	<a href="#">Openbsd</a>	3.5	All	All	All
Operating System	<a href="#">Openbsd</a>	<a href="#">Openbsd</a>	current	All	All	All
Operating System	<a href="#">Openbsd</a>	<a href="#">Openbsd</a>	3.4	All	All	All
Operating System	<a href="#">Openbsd</a>	<a href="#">Openbsd</a>	3.5	All	All	All

Operating System	<a href="#">Openbsd</a>	<a href="#">Openbsd</a>	current	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	2.0	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.4	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.4	All	All	All
Application	<a href="#">Tinysofa</a>	<a href="#">Tinysofa Enterprise Server</a>	1.0	All	All	All
Application	<a href="#">Tinysofa</a>	<a href="#">Tinysofa Enterprise Server</a>	1.0_u1	All	All	All
Application	<a href="#">Tinysofa</a>	<a href="#">Tinysofa Enterprise Server</a>	1.0	All	All	All
Application	<a href="#">Tinysofa</a>	<a href="#">Tinysofa Enterprise Server</a>	1.0_u1	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
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>
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.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>
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>
Apache 'mod_ssl' 'ssl_util_uencode_binary()' Stack Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>
20040605-01-U	SGI	<a href="http://patches.sgi.com">patches.sgi.com</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
'[OpenPKG-SA-2004.026] OpenPKG Security Advisory (apache)' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
2004-0031	TRUSTIX	<a href="http://www.trustix.net">www.trustix.net</a>
Pony Mail!		<a href="http://lists.apache.org">lists.apache.org</a>

Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Gentoo Linux Documentation -- Apache: Buffer overflow in mod_ssl	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
rhn.redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Repository / Oval Repository	OVAL	<a href="https://oval.cisecurity.org">oval.cisecurity.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
[Full-Disclosure] mod_ssl ssl_util_uencode_binary potential problem	FULLDISC	<a href="https://lists.grok.org.uk">lists.grok.org.uk</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
'TSSA-2004-008 - apache' - MARC	BUGTRAQ	<a href="http://marc.info">marc.info</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
redhat.com   Red Hat Support	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
'[security bulletin] SSRT4788 rev. 0 HP-UX Apache Remote arbitrary code execution' - MARC	HP	<a href="http://marc.info">marc.info</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
FLSA:1888	FEDORA	<a href="https://bugzilla.fedora.us">bugzilla.fedora.us</a>
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>
Debian -- Security Information -- DSA-532-2 libapache-mod-ssl	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.0.50: <a href="http://httpd.apache.org/security/vulnerabilities_20.html">http://httpd.apache.org/security/vulnerabilities_20.html</a>

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](#)**