



CVE-2002-0658

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary	
CVE	CVE-2002-0658
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-08-12 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	OSSP mm library (libmm) before 1.2.0 allows the local Apache user to gain privileges via temporary files, possibly via a syn

Risk And Classification	
Primary CVSS:	v2.0 6.2 from nvd@nist.gov
AV:L/AC:H/Au:N/C:C/I:C/A:C	
Problem Types:	NVD-CWE-Other n/a

CVSS v2.0 Breakdown	
Access Vector	Local
Access Complexity	High
Authentication	None
Confidentiality	Complete
Integrity	Complete
Availability	Complete
AV:L/AC:H/Au:N/C:C/I:C/A:C	

NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Ossp	Mm	1.0.0	All	All	All

Application	Ossp	Mm	1.0.1	All	All	All
Application	Ossp	Mm	1.0.10	All	All	All
Application	Ossp	Mm	1.0.11	All	All	All
Application	Ossp	Mm	1.0.12	All	All	All
Application	Ossp	Mm	1.0.2	All	All	All
Application	Ossp	Mm	1.0.3	All	All	All
Application	Ossp	Mm	1.0.4	All	All	All
Application	Ossp	Mm	1.0.5	All	All	All
Application	Ossp	Mm	1.0.6	All	All	All
Application	Ossp	Mm	1.0.7	All	All	All
Application	Ossp	Mm	1.0.8	All	All	All
Application	Ossp	Mm	1.0.9	All	All	All
Application	Ossp	Mm	1.1.0	All	All	All
Application	Ossp	Mm	1.1.1	All	All	All
Application	Ossp	Mm	1.1.2	All	All	All
Application	Ossp	Mm	1.1.3	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference			Source		Link	
SecurityFocus HOME Advisories: Multiple vulnerabilities in OpenSSL and libmm			af854a3a-2127-422b-91ae-364da2661108		online.securityfocus.com	
www.linux-mandrake.com/en/security/2002/MDKSA-2002-045.php			af854a3a-2127-422b-91ae-364da2661108		www.linux-mandrake.com	
Debian -- Security Information -- DSA-137-1 mm			af854a3a-2127-422b-91ae-364da2661108		www.debian.org	
ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SN-02:05.asc			af854a3a-2127-422b-91ae-364da2661108		ftp.freebsd.org	
redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		www.redhat.com	
Security Announcement			af854a3a-2127-422b-91ae-364da2661108		www.novell.com	
redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		www.redhat.com	
ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-032.0.txt			af854a3a-2127-422b-91ae-364da2661108		ftp.caldera.com	
redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		rhn.redhat.com	
ISS X-Force Database: mm-tmpfile-symlink (9719): mm tmpfile symlink attack			af854a3a-2127-422b-91ae-364da2661108		www.iss.net	
rhn.redhat.com/errata/RHSA-2002-156.html			af854a3a-2127-422b-91ae-364da2661108		rhn.redhat.com	
redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		rhn.redhat.com	
redhat.com Red Hat Support			af854a3a-2127-422b-91ae-364da2661108		rhn.redhat.com	
MM Shared Memory Library Temporary File Privilege Escalation Vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.securityfocus.com	

MM Shared Memory Library Temporary File Privilege Escalation vulnerability	a1854a3a-2127-4220-91ae-3b4da2bb1108	www.security.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report