



CVE-2002-0358

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

Summary

CVE	CVE-2002-0358
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-07-26 04:00:00 UTC
Updated	2008-09-05 20:27:00 UTC
Description	MediaMail and MediaMail Pro in SGI IRIX 6.5.16 and earlier allows local users to force the program to dump core via certain

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sgi	Mediamail	All	All	All	All
Application	Sgi	Mediamail	All	All	pro	All
Application	Sgi	Mediamail	All	All	All	All
Application	Sgi	Mediamail	All	All	pro	All

References

Reference	Source	Link
ISS X-Force Database: irix-mediemail-core-dump (9292): SGI IRIX /usr/binX11/MediaMail core dump	XF	www.iss.net
SGI MediaMail Memory Corruption Vulnerability	BID	www.securityfocus.com
20020602-01-I	SGI	patches.sgi.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](#).

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