CVE-2004-0105

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

Summary

CVE	CVE-2004-0105
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-03-03 05:00:00 UTC
Updated	2017-07-11 01:29:00 UTC
Description	Multiple buffer overflows in Metamail 2.7 and earlier allow remote attackers to execute arbitrary code.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Metamail Corporation	Metamail	All	All	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium_processor	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	itanium_processor	All
Application	Sgi	Propack	2.3	All	All	All
Application	Sgi	Propack	2.4	All	All	All
Application	Sgi	Propack	2.3	All	All	All
Application	Sgi	Propack	2.4	All	All	All

References

Reference
IBM X-Force Exchange
'metamail format string bugs and buffer overflows' - MARC

metamail format string bugs and buffer overflows - MARC
VU#513062 - metamail contains multiple buffer overflow vulnerabilities
The Slackware Linux Project: Slackware Security Advisories
Metamail Multiple Buffer Overflow/Format String Handling Vulnerabilities
Advisories - Mandriva
Neohapsis Archives - VulnWatch - #0041 - [VulnWatch] FW: Multiple WinXP kernel vulns can give user mode programs kernel mode privileges
redhat.com | Red Hat Support
Debian -- Security Information -- DSA-449-1 metamail
IBM X-Force Exchange
Secunia - Advisories - Metamail Message Parsing System Compromise Vulnerabilities
O-083: Red Hat Updated Metamail Packages Fix Vulnerabilities
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.

Free CVE JSON API cve.report/api

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