



CVE-2004-1185

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

Summary

CVE	CVE-2004-1185
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-21 05:00:00 UTC
Updated	2018-10-19 15:30:00 UTC
Description	Enscript 1.6.3 does not sanitize filenames, which allows remote attackers or local users to execute arbitrary commands via

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Enscript	1.3.0	All	All	All
Application	Gnu	Enscript	1.4.0	All	All	All
Application	Gnu	Enscript	1.5.0	All	All	All
Application	Gnu	Enscript	1.6.0	All	All	All
Application	Gnu	Enscript	1.6.1	All	All	All
Application	Gnu	Enscript	1.6.2	All	All	All
Application	Gnu	Enscript	1.6.3	All	All	All
Application	Gnu	Enscript	1.3.0	All	All	All
Application	Gnu	Enscript	1.4.0	All	All	All
Application	Gnu	Enscript	1.5.0	All	All	All
Application	Gnu	Enscript	1.6.0	All	All	All
Application	Gnu	Enscript	1.6.1	All	All	All
Application	Gnu	Enscript	1.6.2	All	All	All
Application	Gnu	Enscript	1.6.3	All	All	All

References

Reference

Support
Gentoo Linux Documentation -- enscript: Multiple vulnerabilities
SecurityFocus
SecurityTracker.com Archives - GNU Enscript EPSF and Filename Command Input Validation Errors May Let Remote Users Execute Arbitrar
IBM X-Force Exchange
USN-68-1: enscript vulnerabilities Ubuntu security notices
SecurityFocus
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
About the security content of Security Update 2009-002 / Mac OS X v10.5.7
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities
Debian -- Security Information -- DSA-654-1 enscript
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
GNU Enscript Multiple Vulnerabilities
Repository / Oval Repository
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7
Advisories - Mandriva Linux
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-03-14	Mark J Cox	Red Hat Enterprise Linux 5 is not vulnerable to this issue as it contains a backported patch.

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](#)