



CVE-2003-0101

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

Summary

CVE	CVE-2003-0101
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-03-03 05:00:00 UTC
Updated	2016-10-18 02:29:00 UTC
Description	miniserv.pl in (1) Webmin before 1.070 and (2) Usermin before 1.000 does not properly handle metacharacters such as line

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Engardelinux	Guardian Digital Webtool	1.2	All	All	All
Application	Engardelinux	Guardian Digital Webtool	1.2	All	All	All
Application	Usermin	Usermin	0.4	All	All	All
Application	Usermin	Usermin	0.5	All	All	All
Application	Usermin	Usermin	0.6	All	All	All
Application	Usermin	Usermin	0.7	All	All	All
Application	Usermin	Usermin	0.8	All	All	All
Application	Usermin	Usermin	0.9	All	All	All
Application	Usermin	Usermin	0.91	All	All	All
Application	Usermin	Usermin	0.92	All	All	All
Application	Usermin	Usermin	0.93	All	All	All
Application	Usermin	Usermin	0.94	All	All	All
Application	Usermin	Usermin	0.95	All	All	All
Application	Usermin	Usermin	0.96	All	All	All
Application	Usermin	Usermin	0.97	All	All	All
Application	Usermin	Usermin	0.98	All	All	All
Application	Usermin	Usermin	0.99	All	All	All

Application	Usermin	Usermin	0.4	All	All	All
Application	Usermin	Usermin	0.5	All	All	All
Application	Usermin	Usermin	0.6	All	All	All
Application	Usermin	Usermin	0.7	All	All	All
Application	Usermin	Usermin	0.8	All	All	All
Application	Usermin	Usermin	0.9	All	All	All
Application	Usermin	Usermin	0.91	All	All	All
Application	Usermin	Usermin	0.92	All	All	All
Application	Usermin	Usermin	0.93	All	All	All
Application	Usermin	Usermin	0.94	All	All	All
Application	Usermin	Usermin	0.95	All	All	All
Application	Usermin	Usermin	0.96	All	All	All
Application	Usermin	Usermin	0.97	All	All	All
Application	Usermin	Usermin	0.98	All	All	All
Application	Usermin	Usermin	0.99	All	All	All
Application	Webmin	Webmin	1.0.50	All	All	All
Application	Webmin	Webmin	1.0.60	All	All	All
Application	Webmin	Webmin	1.0.50	All	All	All
Application	Webmin	Webmin	1.0.60	All	All	All

References

Reference

SecureNet Service: SNS Advisory

Secunia - Advisories - Mandrake updates for webmin

Debian -- Security Information -- DSA-319-1 webmin

SecurityTracker.com Archives - Webmin Input Validation Flaw in 'miniserv.pl' May Let Remote Users Spoof Session IDs and Gain Root Access

ISS X-Force Database:webmin-usermin-root-access(11390): Webmin and Usermin session ID spoofing root access

Secunia - Advisories - Webmin Authentication Bypass Vulnerability

Neohapsis Archives - HP Security Digests - #0063 - HP-UX security bulletins digest

LinuxSecurity.com: Gentoo: webmin Unauthorized access vulnerability

Advisories - Mandriva

'Webmin 1.050 - 1.060 remote exploit' - MARC

N-058: Vulnerabilities in Webmin/Usermin

'[SNS Advisory No.62] Webmin/Usermin Session ID Spoofing Vulnerability "Episode 2"' - MARC

'GLSA: usermin (200302-14)' - MARC

Webmin/Usermin Session ID Spoofing Unauthenticated Access Vulnerability

'Webmin version 1.070 released - fixes security hole' - MARC

20030602-01-I

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.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

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