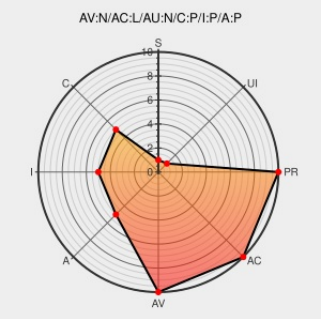
CVE-2005-3912

Published on: 11/30/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-3912

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

Format string vulnerability in miniserv.pl Perl web server in Webmin before 1.250 and Usermin before 1.180, with syslog logging enabled, allows remote attackers to cause a denial of service (crash or memory consumption) and possibly execute arbitrary code via format string specifiers in the username parameter to the login form, which is ultimately used in a syslog call. NOTE: the code execution might be associated with an issue in Perl.

CVE-2005-3912 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityFocus	Third Party Advisory, VDB Entry, www.securityfocus.com, text/html	BUGTRAQ 20051129 Webmin miniserv.pl format string vulnerability
Webmin	Vendor Advisory, www.webmin.com, text/html	CONFIRM www.webmin.com/security.html
Changes since Usermin version 1.170	Vendor Advisory, www.webmin.com, text/plain	CONFIRM www.webmin.com/uchanges-1.180.html

[Dailydave] Webmin miniserv.pl format string vulnerability	Patch Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MLIST [Dailydave] 20051129 Webmin miniserv.pl format string vulnerability
Secunia - Advisories - Webmin "miniserv.pl" Perl Format String Vulnerability	Patch Third Party Advisory web.archive.org text/html	SECUNIA 17749
Debian -- Security Information -- DSA-1199-1 webmin	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-1199
404: Not Found	Patch Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.dyadsecurity.com/webmin-0001.html
Secunia - Advisories - Usermin "miniserv.pl" Perl Format String Vulnerability	Third Party Advisory web.archive.org text/html	SECUNIA 17817
Debian update for webmin - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 22556
Advisories - Mandriva Linux	Third Party Advisory www.mandriva.com text/html	MANDRIVA MDKSA-2005:223
Changes since Webmin version 1.240	Vendor Advisory www.webmin.com text/plain	CONFIRM www.webmin.com/changes-1.250.html
Secunia - Advisories - SUSE Updates for Multiple Packages	Third Party Advisory web.archive.org text/html	SECUNIA 18101
Security Announcement	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2005:030
Secunia - Advisories - Mandriva update for webmin	Third Party Advisory web.archive.org text/html	SECUNIA 17878
Gentoo Linux Documentation -- Webmin, Usermin: Format string vulnerability	Third Party Advisory www.gentoo.org text/html	GENTOO GLSA-200512-02
Gentoo update for webmin/usermin - Advisories - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 17942
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2005-2660

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	3.1	All	All	All
Operating System	Debian	Debian Linux	3.1	All	All	All
Application	Webmin	Webmin	All	All	All	All
Application	Webmin	Webmin	All	All	All	All

cpe:2.3:o:debian:debian_linux:3.1:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:3.1:*:*:*:*:*:*:*:

cpe:2.3:a:webmin:webmin:*:*:*:*:*:*:*:*:

cpe:2.3:a:webmin:webmin:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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