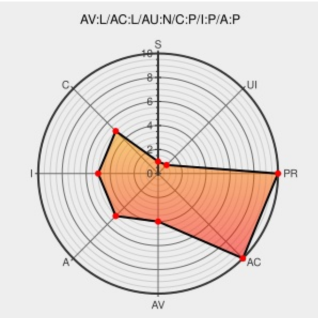
CVE-2002-1165

Published on: 10/03/2002 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1165

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



Certain versions of Netbsd from Netbsd contain the following vulnerability:

Sendmail Consortium's Restricted Shell (SMRSH) in Sendmail 8.12.6, 8.11.6-15, and possibly other versions after 8.11 from 5/19/1998, allows attackers to bypass the intended restrictions of smrsh by inserting additional commands after (1) "||" sequences or (2) "/" characters, which are not properly filtered or verified.

CVE-2002-1165 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
Sendmail Sentrion Open Source - Open Source Email Server | Proofpoint	Exploit, Patch, Vendor Advisory, www.sendmail.org, message/rfc822	CONFIRM www.sendmail.org/smrsh.adv.txt
Sendmail SMRSH Double Pipe Access Validation Vulnerability	Exploit, Patch, Vendor Advisory, cve.report (archive), text/html	BID 5845
No Description Provided	Vendor Advisory, web.archive.org, text/html	XF sendmail-forward-bypass-smrsh(10232)

	Inactive Link Not Archived	
redhat.com | Red Hat Support	www.redhat.com text/html	REDHAT RHSA-2003:073
Home - Conectiva	distro.conectiva.com.br text/html	CONECTIVA CLA-2002:532
Advisories - Mandriva	www.mandriva.com text/html	MANDRIVA MDKSA-2002:083
	ftp.netbsd.org text/plain	NETBSD NetBSD-SA2002-023
No Description Provided	marc.info text/html	BUGTRAQ 20021001 iDEFENSE Security Advisory 10.01.02: Sendmail smrsh bypass vulnerabilities
Secunia - Advisories - IRIX updates to sendmail	web.archive.org text/html	SECUNIA 7826

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 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	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	All	All	All
Operating System	Netbsd	Netbsd	1.5	All	All	All
Operating System	Netbsd	Netbsd	1.5.1	All	All	All
Operating System	Netbsd	Netbsd	1.5.2	All	All	All
Operating System	Netbsd	Netbsd	1.5.3	All	All	All
Operating System	Netbsd	Netbsd	1.6	All	All	All
Application	Sendmail	Sendmail	8.12.0	All	All	All
Application	Sendmail	Sendmail	8.12.1	All	All	All

Application	Sendmail	Sendmail	8.12.2	All	All	All
Application	Sendmail	Sendmail	8.12.3	All	All	All
Application	Sendmail	Sendmail	8.12.4	All	All	All
Application	Sendmail	Sendmail	8.12.5	All	All	All
Application	Sendmail	Sendmail	8.12.6	All	All	All
Application	Sendmail	Sendmail	8.12.0	All	All	All
Application	Sendmail	Sendmail	8.12.1	All	All	All
Application	Sendmail	Sendmail	8.12.2	All	All	All
Application	Sendmail	Sendmail	8.12.3	All	All	All
Application	Sendmail	Sendmail	8.12.4	All	All	All
Application	Sendmail	Sendmail	8.12.5	All	All	All
Application	Sendmail	Sendmail	8.12.6	All	All	All

cpe:2.3:o:netbsd:netbsd:1.5:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.5.1:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.5.2:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.5.3:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.6:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.5:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.5.1:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.5.2:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.5.3:*:*:*:*:*:*:*

cpe:2.3:o:netbsd:netbsd:1.6:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.0:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.1:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.2:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.3:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.4:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.5:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.6:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.0:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.1:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.2:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.3:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.4:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.5:*:*:*:*:*:*:*

cpe:2.3:a:sendmail:sendmail:8.12.6:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→