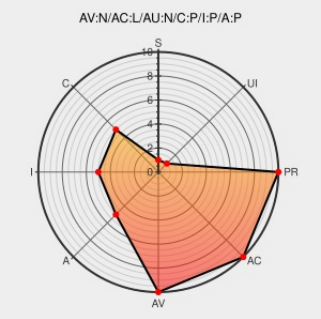
CVE-2004-2771

Published on: 12/24/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:15:00 AM UTC

CVE-2004-2771

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



Certain versions of Bsd Mailx from Bsd Mailx Project contain the following vulnerability:

The expand function in fio.c in Heirloom mailx 12.5 and earlier and BSD mailx 8.1.2 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in an email address.

CVE-2004-2771 has been assigned by secalert@redhat.com 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
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:1999
Security Advisory SA61693 - Oracle Linux update for mailx - Secunia	web.archive.org text/html	SECUNIA 61693
oss-sec: mailx issues (CVE-2004-2771, CVE-2014-7844)	seclists.org text/html	MLIST [oss-security] 20141216 mailx issues (CVE-2004-2771, CVE-2014-7844)
Security Advisory SA60940 - Debian update for heirloom-mailx - Secunia	web.archive.org text/html	SECUNIA 60940
CVE-2004-2771 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2004-2771

Debian -- Security Information -- DSA-3105-1 heirloom-mailx	www.debian.org Depreciated Link text/html	DEBIAN DSA-3105
1162783 – (CVE-2004-2771, CVE-2014-7844) CVE-2004-2771 CVE-2014-7844 mailx: command execution flaw	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1162783
#278748 - mailx: unquoted recipient's name causes sending to fail - Debian Bug report logs	Exploit bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=278748
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:1999
Security Advisory SA61585 - Red Hat update for mailx - Secunia	web.archive.org text/html	SECUNIA 61585
linux.oracle.com | ELSA-2014-1999	linux.oracle.com text/html	CONFIRM linux.oracle.com/errata/ELSA-2014-1999.html

Related QID Numbers

710263 Gentoo Linux mailx Multiple Vulnerabilities (GLSA 201804-06)

901050 Common Base Linux Mariner (CBL-Mariner) Security Update for mailx (6676-1)

901251 Common Base Linux Mariner (CBL-Mariner) Security Update for mailx (7286-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bsd Mailx Project	Bsd Mailx	All	All	All	All
Application	Heirloom	Mailx	All	All	All	All
Operating System	Oracle	Linux	6	All	All	All
Operating System	Oracle	Linux	7	All	All	All
Operating System	Oracle	Linux	6	All	All	All
Operating System	Oracle	Linux	7	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

System						
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

cpe:2.3:a:bsd_mailx_project:bsd_mailx:*:*:*:*:*:*:*:*:
cpe:2.3:a:heirloom:mailx:*:*:*:*:*:*:*:*:
cpe:2.3:o:oracle:linux:6:*:*:*:*:*:*:*:
cpe:2.3:o:oracle:linux:7:*:*:*:*:*:*:*:
cpe:2.3:o:oracle:linux:6:*:*:*:*:*:*:*:
cpe:2.3:o:oracle:linux:7:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→