

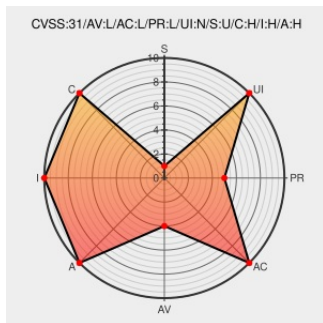


CVE-2014-7844

Published on: 01/14/2020 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:42:00 AM UTC

CVE-2014-7844

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Bsd Mailx](#) from [Bsd Mailx Project](#) contain the following vulnerability:

BSD mailx 8.1.2 and earlier allows remote attackers to execute arbitrary commands via a crafted email address.

CVE-2014-7844 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **BSD - mailx** version = **8.1.2 and earlier**

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
oss-sec: mailx issues (CVE-2004-2771, CVE-2014-7844)	Mailing List Patch Third Party Advisory	MISC seclists.org/oss-sec/2014/q4/1066

	Third Party Advisory seclists.org text/html	
Debian -- Security Information -- DSA-3104-1 bsd-mailx	Third Party Advisory www.debian.org Deprecated Link text/html	 MISC www.debian.org/security/2014/dsa-3104
linux.oracle.com ELSA-2014-1999	Third Party Advisory linux.oracle.com text/html	 MISC linux.oracle.com/errata/ELSA-2014-1999.html
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
CVE-2014-7844 - Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2014-7844
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2014:1999
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 MISC rhn.redhat.com/errata/RHSA-2014-1999.html
Debian -- Security Information -- DSA-3105-1 heirloom-mailx	Third Party Advisory www.debian.org Deprecated Link text/html	 MISC www.debian.org/security/2014/dsa-3105

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.

Related QID Numbers

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bsd Mailx Project	Bsd Mailx	8.1.2	All	All	All
Application	Bsd Mailx Project	Bsd Mailx	8.1.2	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All

System						
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.7	All	All	All
Operating	Redhat	Enterprise Linux Server Eus	6.6	All	All	All

cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server:6.0:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server:7.0:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server:6.0:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server:7.0:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:6.6:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.3:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.7:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:6.6:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.3:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.7:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:6.6:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.3:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.4:***:***:***:
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.5:***:***:***:

```
cpe:2.3:o:redhat:enterprise linux server eus:7.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.7:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:6.6:*.*:*.*:*.:
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.3:::*:*:*.*.*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.6:::*:*:*.*.*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.7::*:~::~
```

```
cpe:2.3:o:redhat:enterprise linux server tus:6.6.*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.3:::*:*:*.*.*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.6:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.7:::*:*:*.*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux workstation:6.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:redhat:enterprise linux workstation:7.0:*.~*~*~*~*~*~*
```

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 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