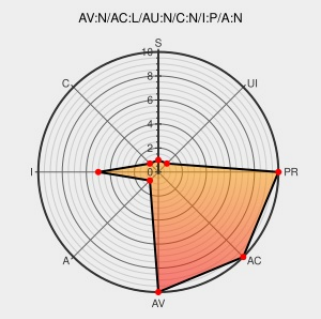
CVE-2006-1251

Published on: 03/18/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1251

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



Certain versions of Sa-exim from Sa-exim contain the following vulnerability:

Argument injection vulnerability in greylistclean.cron in sa-exim 4.2 allows remote attackers to delete arbitrary files via an email with a To field that contains a filename separated by whitespace, which is not quoted when greylistclean.cron provides the argument to the rm command.

CVE-2006-1251 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
#345071 - sa-exim: Potential for deleting arbitrary local files by remote attack - Debian Bug report logs	bugs.debian.org, text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=345071
sa-exim Unauthorized File Access Vulnerability	Patch, cve.report (archive), text/html	BID 17110
Webmail - OVH	Vendor Advisory, www.vupen.com, text/html	VUPEN ADV-2006-0941
sa-exim "greylistclean.cron" File Deletion Vulnerability - Advisories - Secunia	Vendor Advisory, web.archive.org, text/html	SECUNIA 19225

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF saexim-greylistclean-file-deletion(25286)
No Description Provided	Patch marc.merlins.org text/html	CONFIRM marc.merlins.org/linux/exim/files/sa-exim-cvs/Changelog.html

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
Application	Sa-exim	Sa-exim	4.0	All	All	All
Application	Sa-exim	Sa-exim	4.1	All	All	All
Application	Sa-exim	Sa-exim	4.2	All	All	All
Application	Sa-exim	Sa-exim	4.0	All	All	All
Application	Sa-exim	Sa-exim	4.1	All	All	All
Application	Sa-exim	Sa-exim	4.2	All	All	All

cpe:2.3:a:sa-exim:sa-exim:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:sa-exim:sa-exim:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:sa-exim:sa-exim:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:sa-exim:sa-exim:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:sa-exim:sa-exim:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:sa-exim:sa-exim:4.2:*:*:*:*:*:*:*:

← Previous ID

Next ID→