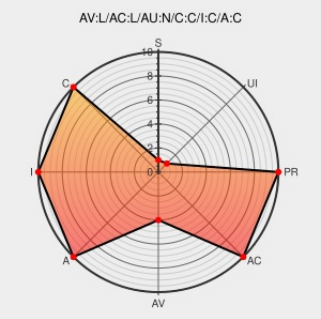
CVE-2005-3346

Published on: 11/20/2005 12:00:00 AM UTC

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

CVE-2005-3346

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



Certain versions of Osh from Osh contain the following vulnerability:

Buffer overflow in the environment variable substitution code in main.c in OSH 1.7-14 allows local users to inject arbitrary environment variables, such as LD_PRELOAD, via pathname arguments of the form "$VAR/EVAR=arg", which cause the EVAR portion to be appended to a buffer returned by a getenv function call.

CVE-2005-3346 has been assigned by security@debian.org to track the vulnerability

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
No Description Provided	pulltheplug.org Inactive Link Not Archived	MISC pulltheplug.org/users/core/files/x_osh3.sh
Debian -- Security Information -- DSA-918-1 osh	www.debian.org Depreciated Link text/html	DEBIAN DSA-918
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF osh-main-execute-code(23091)
Secunia - Advisories - Debian update for osh	web.archive.org text/html	SECUNIA 17967
Secunia - Advisories - osh Environment Variable Substitution Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 17527

Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2005-2378
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 20720
Mike Neuman OSH Environment Variable Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 15370
#338312 - osh: Environment Variable Input Validation Bug - Debian Bug report logs	bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=338312

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	Osh	Osh	1.7.14	All	All	All
Application	Osh	Osh	1.7.14	All	All	All

cpe:2.3:a:osh:osh:1.7.14:*:*:*:*:*:*:*:

cpe:2.3:a:osh:osh:1.7.14:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→