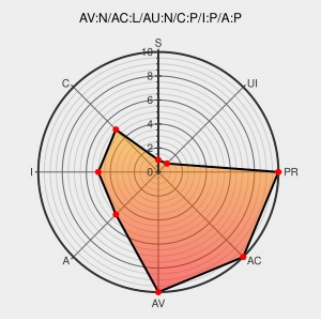
CVE-2005-2661

Published on: 10/14/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:29 PM UTC

CVE-2005-2661

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



Certain versions of Up-imapproxy from Up-imapproxy contain the following vulnerability:

Format string vulnerability in the ParseBannerAndCapability function in main.c for up-imapproxy 1.2.3 and 1.2.4 allows remote IMAP servers to execute arbitrary code via format string specifiers in a banner or capability line.

CVE-2005-2661 has been assigned by security@debian.org 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
Secunia - Advisories - Gentoo update for up-imapproxy	web.archive.org, text/html	SECUNIA 19113
Up-IMAPProxy Multiple Unspecified Remote Format String Vulnerabilities	cve.report (archive), text/html	BID 15048
Debian -- Security Information -- DSA-852-1 up-imapproxy	Patch, Vendor Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN DSA-852
SecurityReason	securityreason.com, text/html	SREASON 547
Secunia - Advisories - Debian update for up-imapproxy	web.archive.org, text/html	SECUNIA 17120

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-2015
Gentoo Linux Documentation -- IMAP Proxy: Format string vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-200603-04
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-2014
Secunia - Advisories - imapproxy "ParseBannerAndCapability" Format String Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 17100

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	Up-imapproxy	Up-imapproxy	1.2.3	All	All	All
Application	Up-imapproxy	Up-imapproxy	1.2.4	All	All	All
Application	Up-imapproxy	Up-imapproxy	1.2.3	All	All	All
Application	Up-imapproxy	Up-imapproxy	1.2.4	All	All	All

cpe:2.3:a:up-imapproxy:up-imapproxy:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:up-imapproxy:up-imapproxy:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:up-imapproxy:up-imapproxy:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:up-imapproxy:up-imapproxy:1.2.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→