



Published on: 06/20/2005 04:00:00 AM UTC

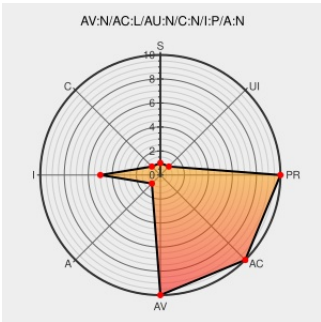
Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2040

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Telnetd](#) from [Telnetd](#) contain the following vulnerability:

Multiple buffer overflows in the `getterminaltype` function in `telnetd` for Heimdal before 0.6.5 may allow remote attackers to execute arbitrary code, a different vulnerability than CVE-2005-0468 and CVE-2005-0469.

CVE-2005-2040 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
Debian -- Security Information -- DSA-758-1 heimdal	www.debian.org Deprecated Link text/html	 DEBIAN DSA-758
2005-06-20: telnetd vulnerabilities	Vendor Advisory web.archive.org text/xml Inactive Link Not Archived	 CONFIRM www.pdc.kth.se/heimdal/advisory/2005-06-20/
Secunia - Advisories - Heimdal telnetd Buffer Overflow Vulnerability	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 15718
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SA:2005:040

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	Telnetd	Telnetd	0.3f	All	All	All
Application	Telnetd	Telnetd	0.4a	All	All	All
Application	Telnetd	Telnetd	0.4b	All	All	All
Application	Telnetd	Telnetd	0.4c	All	All	All
Application	Telnetd	Telnetd	0.4d	All	All	All
Application	Telnetd	Telnetd	0.4e	All	All	All
Application	Telnetd	Telnetd	0.5.0	All	All	All
Application	Telnetd	Telnetd	0.5.1	All	All	All
Application	Telnetd	Telnetd	0.5.2	All	All	All
Application	Telnetd	Telnetd	0.5.3	All	All	All
Application	Telnetd	Telnetd	0.6	All	All	All
Application	Telnetd	Telnetd	0.6.1	All	All	All
Application	Telnetd	Telnetd	0.6.2	All	All	All
Application	Telnetd	Telnetd	0.3f	All	All	All
Application	Telnetd	Telnetd	0.4a	All	All	All
Application	Telnetd	Telnetd	0.4b	All	All	All
Application	Telnetd	Telnetd	0.4c	All	All	All
Application	Telnetd	Telnetd	0.4d	All	All	All
Application	Telnetd	Telnetd	0.4e	All	All	All
Application	Telnetd	Telnetd	0.5.0	All	All	All
Application	Telnetd	Telnetd	0.5.1	All	All	All
Application	Telnetd	Telnetd	0.5.2	All	All	All
Application	Telnetd	Telnetd	0.5.3	All	All	All
Application	Telnetd	Telnetd	0.6	All	All	All
Application	Telnetd	Telnetd	0.6.1	All	All	All
Application	Telnetd	Telnetd	0.6.2	All	All	All

Application	Port(s)	Protocol	CVE ID	CVSS	Exploit	Notes
cpe:2.3:a:telnetd:telnetd:0.3f:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4a:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4b:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4c:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4d:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4e:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.0:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.1:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.2:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.3:*****:*						
cpe:2.3:a:telnetd:telnetd:0.6:*****:*						
cpe:2.3:a:telnetd:telnetd:0.6.1:*****:*						
cpe:2.3:a:telnetd:telnetd:0.6.2:*****:*						
cpe:2.3:a:telnetd:telnetd:0.3f:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4a:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4b:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4c:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4d:*****:*						
cpe:2.3:a:telnetd:telnetd:0.4e:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.0:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.1:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.2:*****:*						
cpe:2.3:a:telnetd:telnetd:0.5.3:*****:*						
cpe:2.3:a:telnetd:telnetd:0.6:*****:*						
cpe:2.3:a:telnetd:telnetd:0.6.1:*****:*						
cpe:2.3:a:telnetd:telnetd:0.6.2:*****:*						

No vendor comments have been submitted for this CVE

© [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](#)