



CVE-2004-1008

Published on: 12/01/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1008

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

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

Integer signedness error in the ssh2_rdpkt function in PuTTY before 0.56 allows remote attackers to execute arbitrary code via a SSH2_MSG_DEBUG packet with a modified stringlen parameter, which leads to a buffer overflow.

CVE-2004-1008 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF putty-ssh2msgdebug-bo\(17886\)](#)

Secunia - Advisories - TortoiseCVS "SSH2_MSG_DEBUG"
Packet Handling Buffer Overflow

[web.archive.org](#)
[text/html](#)

[SECUNIA 13012](#)

IBM notice: The page you requested cannot be displayed

[www-1.ibm.com](#)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM www-1.ibm.com/support/docview.wss?uid=ssg1S1002416](#)

Secunia - Advisories - PuTTY "SSH2_MSG_DEBUG"
Packet Handling Buffer Overflow Vulnerability

[web.archive.org](#)
[text/html](#)

[SECUNIA 12987](#)

'PuTTY SSH client vulnerability' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20041027 PuTTY SSH client vulnerability](#)

Gentoo Linux Documentation -- PuTTY: Pre-authentication

[Patch](#)

[GENTOO GLSA-200410-29](#)

buffer overflow	Vendor Advisory www.gentoo.org text/html	
iDEFENSE : Power Of Intelligence : Current Intelligence : Vulnerabilities	www.idefense.com text/html	 IDEFENSE 20041027 PuTTY SSH2_MSG_DEBUG Buffer Overflow Vulnerability
IBM notice: The page you requested cannot be displayed	www-1.ibm.com text/html Inactive Link Not Archived	 CONFIRM www-1.ibm.com/support/docview.wss?uid=ssg1S1002414
PuTTY: a free telnet/ssh client	www.chiark.greenend.org.uk text/html	 CONFIRM www.chiark.greenend.org.uk/~sgtatham/putty/
PuTTY Remote SSH2_MSG_DEBUG Buffer Overflow Vulnerability	Patch Vendor Advisory cve.report (archive) text/html	 BID 11549
Secunia - Advisories - IBM TotalStorage SAN Volume Controller PuTTY Vulnerability	web.archive.org text/html	 SECUNIA 17214
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	Putty	Putty	0.48	All	All	All
Application	Putty	Putty	0.49	All	All	All
Application	Putty	Putty	0.50	All	All	All
Application	Putty	Putty	0.51	All	All	All
Application	Putty	Putty	0.52	All	All	All
Application	Putty	Putty	0.53	All	All	All
Application	Putty	Putty	0.53b	All	All	All
Application	Putty	Putty	0.54	All	All	All
Application	Putty	Putty	0.55	All	All	All
Application	Putty	Putty	0.48	All	All	All
Application	Putty	Putty	0.49	All	All	All
Application	Putty	Putty	0.50	All	All	All
Application	Putty	Putty	0.51	All	All	All
Application	Putty	Putty	0.52	All	All	All
Application	Putty	Putty	0.53	All	All	All
Application	Putty	Putty	0.53b	All	All	All

Application	Putty	Putty	0.54	All	All	All
Application	Putty	Putty	0.55	All	All	All
Application	TortoiseCVS	TortoiseCVS	1.8	All	All	All
Application	TortoiseCVS	TortoiseCVS	1.8	All	All	All
cpe:2.3:a:putty:putty:0.48:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.49:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.50:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.51:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.52:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.53:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.53b:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.54:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.55:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.48:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.49:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.50:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.51:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.52:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.53:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.53b:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.54:*:*:*:*:*:						
cpe:2.3:a:putty:putty:0.55:*:*:*:*:*:						
cpe:2.3:a:tortoiseCVS:tortoiseCVS:1.8:*:*:*:*:*:						
cpe:2.3:a:tortoiseCVS:tortoiseCVS:1.8:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)