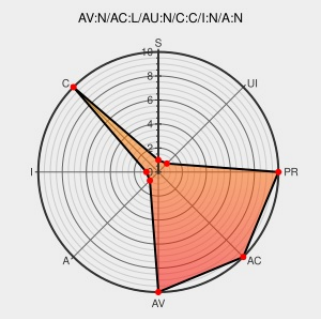
CVE-2011-4722

Published on: 12/27/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:12 PM UTC

CVE-2011-4722

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



Certain versions of Tftp Server from Ipswitch contain the following vulnerability:

Directory traversal vulnerability in the TFTP Server 1.0.0.24 in Ipswitch WhatsUp Gold allows remote attackers to read arbitrary files via a .. (dot dot) in the Filename field of an RRQ operation.

CVE-2011-4722 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ipswitch-tftp-directory-traversal(71610)
SecPod Research Blog » Ipswitch TFTP Server Directory Traversal Vulnerability	Exploit secpod.org text/x-python Inactive Link Not Archived	MISC secpod.org/blog/?p=424
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 77455
Ipswitch TFTP Server Directory Traversal Vulnerability	Exploit www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 18189

Ipswitch WhatsUp TFTP Server Input Validation Flaw Lets Remote Users Traverse the Directory - SecurityTracker	securitytracker.com text/html	SECTRACK 1026368
Software and Drivers	h20565.www2.hp.com text/html	HP HPSBGN3547
About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 47025

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	Ipswitch	Tftp Server	1.0.0.24	All	All	All
Application	Ipswitch	Tftp Server	1.0.0.24	All	All	All

cpe:2.3:a:ipswitch:tftp_server:1.0.0.24:*:*:*:*:*:*:*

cpe:2.3:a:ipswitch:tftp_server:1.0.0.24:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→