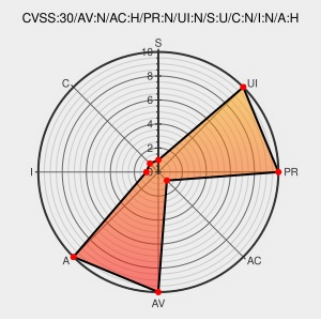
CVE-2017-15271

Published on: 11/15/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:33 PM UTC

CVE-2017-15271

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



Certain versions of Psftpd from Psftp contain the following vulnerability:

A use-after-free issue could be triggered remotely in the SFTP component of PSFTPd 10.0.4 Build 729. This issue could be triggered prior to authentication. The PSFTPd server did not automatically restart, which enabled attackers to perform a very effective DoS attack against this service. By sending a crafted SSH identification / version string to the server, a NULL pointer dereference could be caused, apparently because of a race condition in the window message handling, performing the cleanup for invalid connections. This incorrect cleanup code has a use-after-free.

CVE-2017-15271 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Advisory: X41-2017-006: Multiple Vulnerabilities in	Third Party Advisory	MISC www.x41-dsec.de/lab/advisories/x41-2017-006

Advisory X41-2017-006: Multiple Vulnerabilities in PSFTPd Windows FTP server | X41 D-SEC GmbH	Third Party Advisory www.x41-dsec.de text/html	MISC www.x41-dsec.de/lab/advisories/x41-2017-006-psftpd/
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20171110 Advisory X41-2017-006: Multiple Vulnerabilities in PSFTPd Windows FTP Server
PSFTPd Windows FTP Server 10.0.4 Build 729 Use-After-Free / Log Injection ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/144972/PSFTPd-Windows-FTP-Server-10.0.4-Build-729-Use-After-Free-Log-Injection.html
PSFTPd Windows FTP Server 10.0.4 Build 729 - Log Injection / Use-After-Free - Windows dos Exploit	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43144

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	Psftp	Psftpd	10.0.4	All	All	All
Application	Psftp	Psftpd	10.0.4	All	All	All

cpe:2.3:a:psftp:psftpd:10.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:psftp:psftpd:10.0.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© 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 registred 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