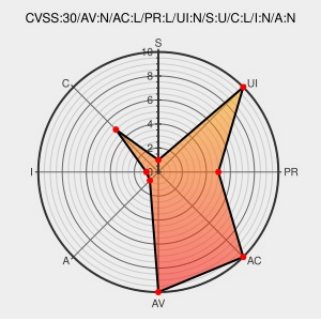
CVE-2017-15269

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

Last Modified on: 03/23/2021 11:26:34 PM UTC

CVE-2017-15269

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



Certain versions of Psftpd from Psftp contain the following vulnerability:

The PSFTPd 10.0.4 Build 729 server does not prevent FTP bounce scans by default. These can be performed using "nmap -b" and allow performing scans via the FTP server.

CVE-2017-15269 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
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	BUGTRAQ 20171110 Advisory X41-2017-006:

	text/html	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

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→