ProFTPD remote code execution vulnerability affects more than 1 million servers worldwide

More than 1 million is the number of ProFTPD servers that are vulnerable to remote code execution worldwide.

More than 1 million is the number of ProFTPD servers that are vulnerable to remote code execution, as well as being the target of information theft attacks, activated after the exploit successfully exploits the vulnerability. Copy files arbitrarily.

If you don't know, ProFTPd is a cross-platform FTP server, and at the same time acts as an open source system that can support most current UNIX-like and Windows systems. In fact, ProFTPd is one of the most commonly used servers targeting UNIX-based platforms, along with Pure-FTPd and vsftpd.

The vulnerability allows remote code collection to run on more than 1 million ProFTPd servers

All ProFTPd versions taken into account (and included) 1.3.5b are said to be affected by a security vulnerability that allows an attacker to execute arbitrary remote code without having to authenticate, together That is the privilege of ProFTPD service after they successfully exploit this vulnerability.

1. If you are using Logitech keyboard, mouse, you need to update the firmware immediately

ProFTPd 1.3.6 was released to patch the vulnerability

The above security vulnerability is currently being tracked under the code name CVE-2019-12815 (Debian, SUSE, Ubuntu), and has been identified in the mod_copy module by security expert Tobias Mädel. This

vulnerability was of course reported to ProFTPd's security team. Shortly thereafter, the ProFTPd 1.3.6 version was also quickly released on July 17 as an additional security patch.

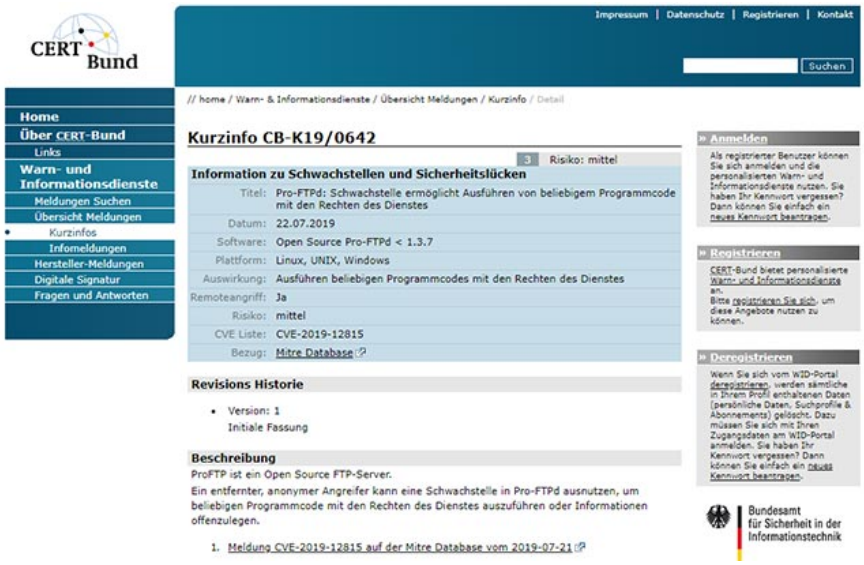
Mädel's description of the incorrect access control error is as follows: "mod_copy is provided in the default installation of ProFTPd, and is also enabled by default in most distributions (such as like Debian) Issuing CPFR and CPTO commands for ProFTPd servers allows users who do not own write rights (write permissions), can copy any file on the FTP server ".

1. Video software calls for a dangerous vulnerability that allows the bad guys to easily turn on the MacBook webcam without your knowledge

According to the information obtained from ProFTPd's bug tracker system, the problem occurred stemming from "the customized SITE CPFR and SITE CPTO commands of the mod_copy module are not arranged and configured as expected".

In case the server administrator cannot install the ProFTPd 1.3.5 release immediately to prevent potential attacks, it is possible to disable the mod_copy module in the ProFTPd configuration file as a solution. decision is relatively effective situation.

CERT-Bund - Germany's emergency response team for computer problems (Computer Emergency Response Team) - recently released a confidential recommendation on July 22 to alert ProFTPD users. about this potentially serious vulnerability.



Security recommendations of the CERT-Bund team

Another noteworthy information is that an arbitrary file copying hole found in the mod_copy module of ProFTPD as of version 1.3.5b is closely related to another security error. identifier CVE-2015-3306 was discovered since 2015, allowing an attacker to perform read and write operations to arbitrary files remotely using only the 'SITE CPFR' and 'SITE CPTO' commands. .

1. Hundreds of millions of Windows 10 computers are easily hacked due to errors in the original software of the manufacturer

More than one million ProFTPd servers have not been patched for security

According to the Shodan security organization, there are currently more than 1 million ProFTPd servers worldwide that have not been updated to the latest patch, while only 4 servers have been upgraded since that time. ProFTPd 1.3.6 fixed version is officially released - an alarming difference.

List and partition number of ProFTPd servers vulnerable to worldwide attack

The large number of vulnerable servers is thus more likely to make this vulnerability an attractive target for attackers in the future. The script is still very familiar, bad actors will use more exciting exploits to infiltrate the system and infect malicious code on all servers that have not been updated to the latest patch.

Currently hackers are primarily targeting vulnerable Jira and Exim servers, as well as infecting these servers with a new Watchbog Linux Trojan variant, with the resulting botnet used to exploit Monero electronic money. .

1. Appearing a zero-day vulnerability in Firefox, Mozilla advises users to update to the latest version immediately

That the Jira CVE-2019-11581 sample injection hole that these attackers are targeting has been publicly disclosed just 12 days ago is evidence that the speed at which agents threaten to start abusing those How new security vulnerabilities are becoming worrying.