Miscellaneous

Additional and miscellaneous information, often requested by users and customers, but that wouldn't fit in any specific knowledge base category.

- No, we are not affected by Log4j vulnerability (CVE-2021-44228)
- How Syncplify.me Server! prevents SSHPsycho attacks
- W3C log file format and UTC timestamps
- Firewalls and FTP external IP address for PASV
- Where do I download the old v4/v5 installers?

No, we are not affected by Log4j vulnerability (CVE-2021-44228)

No Syncplify software uses (nor has ever used) anything written in Java. Furthermore, and more specifically, no Syncplify software uses (nor has ever used) Log4j. Therefore, none of our software is affected by (nor it has ever been) any Log4j bug or vulnerability.

How Syncplify.me Server! prevents SSHPsycho attacks

According to the SANS ISC nearly 80% of all SSH-based brute force attacks are caused by SSHPsycho or one of its variants. This seems to be confirmed by the LongTail honeypot real-time report provided by the Marist College. So, yes, SSHPsycho is a big deal, and it's a problem. And traditional blacklisting mechanisms (simply banning certain "well known" IP addresses and networks) have proved to be inefficient against it.

> "LongTail shows that Cisco and Level 3's recent announcement about blocking sshPsycho's 4 class C IP ranges (also known as "Group 93" and the "Hee Thai Campaign") has done nothing to stop their brutal attacks. [Source: SANS ISC]"

Syncplify.me Server!'s intelligent and automatic blacklist (called "**Protector**"), though, shows to be **extremely effective at preventing** such type of attack. Its real-time dynamic attack pattern identification and prevention technology can quickly recognize SSHPsycho attacks (and the like) and **proactively stop them** as soon as they begin. Even at its "Normal" sensitivity threshold, Protector already identifies and blocks all types of SSHPsycho attacks, in most cases **before they even get to try the password authentication**.

Of course, not even Protector can keep you safe if you have a user whose username is "*test*" and its password is "*123456*", so it's strongly recommended to read the LongTail report and **avoid using the most common username/password combinations** that would make your SSH/SFTP server inherently vulnerable, not only to SSHPsycho but pretty much to any known and unknown attack. But again, Syncplify.me Server! helps you by **enforcing password complexity rules** that prevent users from using passwords that would be too easy to guess.

W3C log file format and UTC timestamps

Every once in a while we receive a support request from some customers asking us how to **“fix” the timestamp** in the log files because it’s few hours ahead/behind.

The thing is that such timestamp is not ahead nor behind: it’s always in UTC (Coordinated Universal Time), and that is not our arbitrary choice; in fact, the W3C Extended Log File Format official working document clearly states that the timestamp **must** refer to the GMT time zone without daylight savings bias, which is – indeed – called UTC for brevity.

For such reason, all existing log analysis software products are designed to take that into account and adapt the generated reports to the current time zone of the machine that runs the analysis.

There are tens of log analysis software titles out there, but since sometimes our users ask us for a recommendation, here’s two among our favorites:

- Sawmill
- SmarterStats

Both of them are very high-quality products, and have been tested and confirmed to work flawlessly with the log files products by Syncplify.me Server!

Firewalls and FTP external IP address for PASV

Most firewalls (we'd say all the ones we know) have NAT/PAT capabilities, and many are able to perform a protocol-level inspection when the connection is not encrypted. SSH (and SFTP) are always encrypted, but FTP can be either encrypted or not; yet, theoretically, **protocol inspection should only prevent protocol-related attacks, not modify client requests or server responses.**

Yet, one customer with a perfectly configured instance of Syncplify Server! reported experiencing a **weird behavior**: FTPS/FTPES (encrypted) sessions were working perfectly, while plain FTP sessions were dropped upon every attempt to open a data connection to transfer files.

Now, theoretically, this doesn't make any sense, as the core engine for the FTP protocol is the same, and the TLS channel is layered on top of (or, more precisely, encapsulates) it. The only possible explanation was that something between the client and the server **was actively modifying the protocol**, and could obviously do so only when the FTP connection was performed in clear, with no TLS encryption.

In this particular case, a SonicWall firewall was **rewriting Syncplify Server!'s response to the PASV command** in order to modify the IP address and Port for the next incoming (requested) passive data connection.

Now, Syncplify Server! – as most FTP/S servers – allows the server's administrator to configure an "*external IP for PASV connections*" to be used specifically when running our server behind NAT/PAT. This allows the server to tell the client to which public IP:Port it should connect to initiate the data transfer connection. If the firewall rewrites such information and re-routes the data connection towards a different IP or Port, then Syncplify Server! would **not accept the new incoming data connection request, because it is – de facto – tampered or spoofed**.

If you have a firewall that acts like this (more like a reverse proxy, rather than just a simple firewall) removing the "*external IP for PASV connections*" from Syncplify Server!'s configuration **may fix the issue**, as it did in our example case. But please keep in mind that such a configuration setting is there for a reason, and if your firewall is behaving transparently it is necessary to use it when behind NAT/PAT.

Where do I download the old v4/v5 installers?

> **WARNING**: both *version 4* and *version 5* are now discontinued and retired, so please be aware that downloading the following installers comes with no guarantee of support or fitness-for-purpose of any kind. **Syncplify, Inc. is also not liable for any malfunction or damages these versions of the software may cause, for any reason, to the maximum extent permitted by law. If you continue, you take full responsibility, and do so at your own risk.**

Download: version 4.2.5 installer

Download: version 5.1.30 installer