FileZilla® refocuses on security after participation in EU bug bounty program

EU program found some security issues, which FileZilla has promptly fixed

KöLN, GERMANY, July 29, 2019 /EINPresswire.com/ -- FileZilla®, the cross-platform file access and transfer software application, has quickly solved some security issues identified in the recent participation in the European Union-sponsored “bug bounty” program.

> “Security is paramount for FileZilla; even the smallest anomalies get fixed promptly. We will continue our vigilance to provide excellent security as we continue to expand our products and services.”
>
> *Tim Kosse*

FileZilla began participating in the bug bounty in January 2019. The European Union’s Free and Open Source Software Auditing (EU-FOSSA) project was created in 2015 by the European Parliament to test and improve the security and reliability of open source software that the European Union institutions use. The program, run by the European Commission, paid researchers to find bugs and vulnerabilities.

Previous EU-FOSSA deliverables enlisted all open source programs that are potentially critical due to their presence and use at the European Institutions, and FileZilla made it to the EU’s OSS shortlist ranking.

The EU-FOSSA program found some security issues in FileZilla’s infrastructure, which FileZilla quickly corrected. “We appreciated the opportunity to be part of this program,” said Tim Kosse, FileZilla Founder and Team Leader. “Participation in the program reflects the high priority FileZilla has always placed on security for its users,” Kosse said. FileZilla will continue to make security a high priority as its products get enhanced, he said.

Open source software is the backbone of the internet," said Shlomie Liberow, technical program manager II for the EU-FOSSA programs at HackerOne. "The benefits of the European Commission's sponsorship of bug bounty programs for open source projects through EU-FOSSA extends far beyond the projects involved. Every vulnerability identified was properly and very promptly, fixed by FileZilla, contributing to a safer internet for all.”

To build on the EU-FOSSA experience, FileZilla will continue to run bug bounties, said FileZilla Director of Strategy Roberto Galoppini. “FileZilla will run those tests by investing revenues from FileZilla Pro products to provide the highest level of security to both FileZilla users and FileZilla Pro customers,” Galoppini said.

Kosse outlined some specific bugs that were analyzed and fixed:

1. When opening a file in an editor, filenames containing double-quotation marks were not escaped correctly, resulting in the wrong arguments being passed to the editor. Depending on the associated editor, these arguments could have been interpreted as commands instead of filenames. New versions of FileZilla and FileZilla Pro with fix for this high severity issue were released across all platforms in under 24 hours since the initial bug report.

2. Bug bounty found an assertion when a server sent directory listings with immensely huge file sizes. The risk from this assertion was an ordinary crash.

3. FileZilla was looking for its helper tools and data files in directories in the wrong places or in the wrong order. The FileZilla team made the search paths more strict to correct this flaw. This issue did not affect ordinary installations. Furthermore, there are two preconditions for this issue to be a problem: The user has to interfere with the structure of FileZilla's program files, or an attacker must place new files on the local system. The latter problem is an uncommon condition because the computer would need to be already compromised.

4. Researchers found a buffer-overread (which can violate memory safety) occurred if a custom external IP address resolver sent invalid chunk sizes. Apart from possibly crashing, nothing bad happens. The functionality the bug is not even enabled by default.

5. Some popular operating systems struggle with long menu labels, resulting in visual artifacts. FileZilla now limits the length of site and bookmark names that the user can enter. This is an ordinary bug with no security impact.

6. FileZilla learned that libstdc++, an implementation of the C++ Standard Library, uses a recursive parser for regular expressions. However, even moderately large regular expressions can lead to a crash due to stack exhaustion. FileZilla solved this problem by limiting the regular expression length the user can enter in search and filter conditions. Again, this bug has no security impact.

7. Importing queue files with missing elements could trigger an assertion. FileZilla now ignores the invalid items. This bug has no security impact.

“We are proud to have participated in the bug bounty program,” Kosse said. “Security is paramount for FileZilla; even the smallest anomalies get fixed promptly. We will continue our vigilance to provide excellent security as we continue to expand our products and services,” he said.

About FileZilla Pro
FileZilla Pro allows system administrators, Web developers, designers, and other professional users to transfer files across all types of remote servers and computing environments. For more information about FileZilla Pro services, visit https://filezillapro.com.

Roberto Galoppini
FileZilla Project
+1 315-510-5172
email us here
Visit us on social media:
Facebook
Twitter