

## CVE-2023-42657 WS\_FTP Server

### Summary:

CVE-2023-42657 is a critical vulnerability in WS\_FTP Server, a file transfer software developed by Progress Software. It is a directory traversal vulnerability that allows an attacker to access and modify files and folders outside of their authorised WS\_FTP folder path, as well as on the underlying operating system. It affects WS\_FTP Server versions prior to 8.7.4 and 8.8.2<sup>1</sup>, which means it is very severe and can cause high impact on the confidentiality, integrity and availability of the system.

### Severity:

CVSS score
9.9

### Analyst Assessment:

The attackers may use these techniques to delete, rename, create or modify files and folders on the server or the operating system, which could lead to data loss, corruption, or encryption by ransomware. They may also use the compromised server as a foothold to launch further attacks on the network.

This vulnerability is being exploited in the wild by ransomware hackers who can access and modify files and folders outside of their authorized WS\_FTP folder path, as well as on the underlying operating system.

Some of the reported attack vectors include:

- Sending malicious requests to the WS\_FTP Server's web interface that contain specially crafted parameters that allow the attacker to traverse the directory structure and execute commands on the server.
- Using a valid username and password to log in to the WS\_FTP Server and then sending requests that include ".../" sequences to access files and folders outside of the user's home directory.
- Exploiting another vulnerability, CVE-2023-40044, which is a .NET deserialization vulnerability that allows unauthenticated remote code execution, and then using CVE-2023-42657 to perform further actions on the compromised server.

### Observation:

In all WS\_FTP Server versions prior to 8.7.4 and 8.8.2, a directory traversal vulnerability was discovered. An attacker could leverage this vulnerability to perform file operations (delete, rename, rmdir, mkdir) on files and folders outside of their authorized WS\_FTP folder path. Attackers could also escape the context of the WS\_FTP Server file structure and perform the same level of operations (delete, rename, rmdir, mkdir) on file and folder locations on the underlying operating system.

**Issue Correction:**

Progress Software has released security updates to address this vulnerability, as well as other vulnerabilities found in WS\_FTP Server. Users are advised to apply the updates as soon as possible to prevent potential exploitation by malicious actors. You can find more information about the updates and how to install them on the Progress website.

Customers should make sure they only download the patch from our knowledge base and not from any third-party sites.

Upgrading to a patched release, using the full installer, is the only way to remediate this issue.

**Caveat:**

This is based on current, limited knowledge, which should be further investigated and checked, before being applied to your systems.

**Sources:**

1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42657>
2. [NVD - CVE-2023-42657 \(nist.gov\)](#)
3. [Progress Issues Security Update for Critical Vulnerabilities in WS\\_FTP Server - NHS Digital](#)
4. [WS\\_FTP - Secure FTP Server and Client Software - Progress](#)