10 years CERT-EU

Security Advisory 2023-070

Critical Vulnerabilities in Progress WS_FTP Server Software

September 29, 2023 — v1.0

TLP:CLEAR

History:

- *29/09/2023 — v1.0 – Initial publication*

Summary

On September 27, Progress Software released an advisory announcing multiple vulnerabilities in its enterprise-grade WS_FTP Server secure file transfer software. Two of the vulnerabilities, identified by `CVE-2023-40044` and `CVE-2023-42657`, are rated as **critical**. These flaws expose systems to unauthenticated remote command execution and directory traversal attacks. Immediate patching is strongly advised.

Technical Details

The vulnerability `CVE-2023-40044` is a .NET deserialisation flaw within the Ad Hoc Transfer module. Successful exploitation allows unauthenticated attackers to execute arbitrary remote commands.

The second critical vulnerability, `CVE-2023-42657`, is a directory traversal vulnerability. Attackers can exploit this flaw to conduct file operations outside the authorised WS_FTP folder path, affecting the underlying operating system.

Both vulnerabilities have a CVSS:3.1 rating that indicates low-complexity attacks which do not require user interaction for successful exploitation.

Affected Products

The vulnerabilities specifically impact the software's manager interface and Ad hoc Transfer Module in all versions prior to 8.8.2. Users of WS_FTP Server across various IT sectors worldwide are affected.

Recommendations

Progress Software has addressed these issues in version 8.8.2 of the WS_FTP Server software. Upgrading to this version using the full installer is the only method for remediation. An outage will be expected during the upgrade process.

For users not utilising the Ad Hoc Transfer module, Progress Software has provided instructions to remove or disable this vulnerable feature.

Additional Context

This security advisory comes in the wake of Progress Software grappling with extensive data theft attacks, exploiting a zero-day vulnerability in their MOVEit Transfer platform. These attacks, mainly orchestrated by the Clop ransomware gang, have affected more than 2100 organizations and over 62 million individuals. Despite the high ransom demands, only a limited number of victims are likely to pay, although the financial impact is estimated to be between $75 million and $100 million.

References

[1] https://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023