September 29, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a Progress WS_FTP Server vulnerability. The WS_FTP team discovered vulnerabilities in the WS_FTP Server Ad hoc Transfer Module and in the WS_FTP Server manager interface. All versions of WS_FTP Server are affected by these vulnerabilities.

Technical Details

The critical vulnerabilities discovered impact the WS_FTP Server versions prior to 8.7.4 and 8.8.2, a pre-authenticated attacker could leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system. Additionally, 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.

Also discovered were significant high vulnerabilities in a reflected cross-site scripting (XSS) vulnerability exists in WS_FTP Server's Ad Hoc Transfer module. An attacker could leverage this vulnerability to target WS_FTP Server users with a specialized payload which results in the execution of malicious JavaScript within the context of the victim's browser. SQL injection high vulnerability exists in the WS_FTP Server manager interface. An attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address this risk.

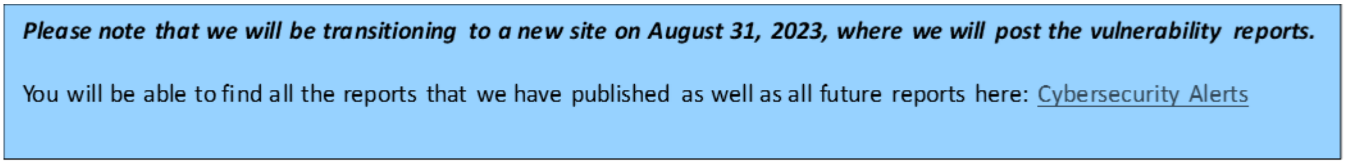
Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-40044, CVE-2023-42657, CVE-2023-40045, CVE-2023-40046, CVE-2023-40047, CVE-2023-40048, CVE-2023-40049, CVE-2022-27665
- WS_FTP Server Critical Vulnerability - (September 2023),



Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts