VULNERABILITY BULLETINS

WS_FTP Critical Vulnerability

TLP:WHITE

Sep 29, 2023

Summary:

On September 09, 2023, Progress Software released a hotfix to address multiple critical vulnerabilities in the WS_FTP Server and the WS_FTP Server Ad hoc Transfer Module. If left unpatched, these vulnerabilities could allow attackers to remotely execute code on the devices and perform file operations outside of the authorized WS_FTP folder paths. The following vulnerabilities have been tracked through multiple CVEs:

- CVE-2023-42657 (CVSS 9.9)
- CVE-2023-27665 (CVSS 6.1)
- CVE-2023-40044 (CVSS 10)
- CVE-2023-40449 (CVSS 5.3)

BlueVoyant has provided a list of Health-ISAC member organizations that are potentially vulnerable to the latest critical vulnerability in the WS_FTP Server Ad hoc Transfer Module and in the WS_FTP Server Manager interface.

Targeted Alerts are being provided to the organizations where Health-ISAC has visibility into the usage of Progress WS_FTP.

Vulnerability Details:

According to Progress Software, all versions of WS_FTP Server are affected by these vulnerabilities. Progress Software has addressed these issues and made version-specific hotfixes available for customers to remediate.

For customers who only have the Ad Hoc Module of WS_FTP installed, Progress Software offers mitigation instructions here. The eight CVEs released by Progress Software fall into three categories. CVEs 2023-40044 and 2023-42657 are considered critical, with CVSS scores of 10 and 9.9, respectively. The other six CVEs have been categorized as high and medium.

CVE-2023-40044 received a maximum 10/10 severity rating as an unauthenticated attacker could execute remote commands after successfully exploiting a .NET deserialization vulnerability in the Ad Hoc Transfer module. The other critical vulnerability (CVE-2023-42657) is a directory traversal vulnerability, enabling an attacker to perform file operations outside the authorized WS_FTP folder path.

Recommendations:

BlueVoyant recommends all clients running any of the affected versions listed above to perform a business impact study and apply the appropriate updates immediately. Progress Software highly recommends you upgrade to a supported version of the products.

Reference(s)	Progress, Bleeping Computer, The Record, The Hacker News

Release Date
Sep 30, 2023 (UTC)

Alert ID 24344b13

View Alert

Tags Critical Vulnerabilities, Progress

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits

https://h-isac.org/events/

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP "Share Threat Intel" Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Knowledge Base

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

Access the Health-ISAC Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**