Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

September 29, 2023 TLP:CLEAR Report: 202309291500

Progress Software WS_FTP Critical Vulnerabilities

Executive Summary

Progress Software, the maker of the MOVEit file transfer software which was widely exploited by the CLOP ransomware-as-a-service (Raas) group, has released a new advisory regarding multiple vulnerabilities in the WS_FTP Server, a file transfer product. Two of the vulnerabilities were rated as critical and are being tracked as CVE-2023-40044, which can allow an attacker to execute remote commands, and as CVE-2023-4265, which is a directory traversal vulnerability. Due the recent and malicious targeting of Progress Software's products to compromise Healthcare and Public Health (HPH) sector entities, HC3 strongly encourages patching and upgrading these devices to prevent serious damage to the HPH sector.

Report

On September 27, 2023, Progress Software released an advisory regarding multiple vulnerabilities in their globally-used file transfer software, the WS_FTP Server. WS_FTP is reportedly used by thousands of IT teams, and two new critical vulnerabilities have been identified within it. The vulnerabilities are being tracked as CVE-2023-40044 and CVE-2023-4265. CVE-2023-40044 affects versions prior to 8.7.4 and 8.8.2, allowing a pre-authenticated attacker to leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system. CVE-2023-4265 is a directory traversal vulnerability that impacts the same versions. If successfully exploited, an attacker could leverage this to perform file operations (delete, rename, rmdir, mkdir) on files and folders that are outside of the authorized WS_FTP path. Additionally, the attacker could escape the WS_FTP server file structure and perform the same operations on the operating system. The remaining reported vulnerabilities are listed below:

- **CVE-2023-40045 (CVSS 8.3):** Reflected XSS in the WS_FTP Server's Ad Hoc Transfer module
- **CVE-2023-40046 (CVSS 8.2)**: SQL injection vulnerability in the WS_FTP Server manager interface
- **CVE-2023-40047 (CVSS 8.3)**: Stored XSS vulnerability in WS_FTP Server's Management module
- **CVE-2023-40048 (CVSS 6.8)**: Cross-site request forgery vulnerability in WS_FTP
- **CVE-2022-27665 (CVSS 6.1)**: Reflected XSS in Progress Ipswitch WS_FTP Server 8.6.0
- **CVE-2023-40049 (CVSS 5.3)**: File enumeration vulnerability in the 'WebServiceHost' directory

The advisory, along with further details of the newly discovered vulnerabilities, can be found here:

- WS_FTP Server Critical Vulnerability - (September 2023) - Progress Community

Recent operations conducted from the CLOP ransomware group, which are believed to have started in May 2023, actively targeted a zero-day vulnerability in Progress Software's MOVEit file transfer application. The vulnerability is tracked as CVE-2023-34362 and the group was successfully able to compromise thousands of organizations worldwide, including the healthcare sector.

Patches, Mitigations, and Workarounds

HC3 strongly encourages all users to follow the manufacturer's recommendation and upgrade to the highest version available (8.8.2) to prevent any damage from occuring against the HPH sector. Organizations that are not able to update immediately can still disable the WS_FTP Server Ad hoc Transfer Module by following the article below:

- Removing or Disabling the WS_FTP Server Ad hoc Transfer Module - Progress Community

Related Reports

- 202306161700_Critical Vulnerability in MOVEit Transfer Software Sector Alert_TLPCLEAR (hhs.gov)
- 202306021200_Critical Vulnerability in MOVEit Transfer Software Sector Alert_TLPCLEAR (hhs.gov)
- 202304281500_Cl0p and Lockbit New Data Breaches Sector Alert_TLPCLEAR (hhs.gov)

References

Gatlan, Sergiu. Progress warns of maximum severity WS_FTP Server vulnerability. Bleeping Computer. September 28, 2023. Progress warns of maximum severity WS_FTP Server vulnerability (bleepingcomputer.com)

Progress Community. WS_FTP Server Critical Vulnerability - (September 2023). September 27, 2023. WS_FTP Server Critical Vulnerability - (September 2023) - Progress Community

Progress Community. Removing or Disabling the WS_FTP Server Ad hoc Transfer Module. September 27, 2023. Removing or Disabling the WS_FTP Server Ad hoc Transfer Module - Progress Community

CVE Records. CVE-2023-40044. September 27, 2023. CVE Record | CVE

CVE Records. CVE-2023-42657. September 27, 2023. CVE Record | CVE

NIST. CVE-2023-34362. June 23, 2023. NVD - CVE-2023-34362 (nist.gov)

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback