National Cyber Security Centre

2309290111-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Multiple Critical Vulnerabilities in WS_FTP Server

Monday 2nd October, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Revision History

Revision	Date	Author(s)	Description
1.0	29th Septemper 2023	CSIRT-IE	Initial advisory responding to Progress advisory
1.1	02nd October 2023	CSIRT-IE	Update with details of POC and exploitation.

Description

Progress has released details about multiple vulnerabilities that exist in WS_FTP server. The vulnerabilities exist within the WS_FTP Server Ad Hoc Transfer Module and the WS_FTP Server manager interface. Two of these vulnerabilities are rated as critical, the remaining vulnerabilities are rated high and medium.

CVE-2023-40044 with a CVSS rating of 10, is a critical vulnerability that exists within WS_FTP Server versions prior to 8.7.4 and 8.8.2 and could allow a pre-authenticated attacker to leverage a .NET deserialisation vulnerability in the Ad Hoc Transfer Module to execute remote commands on the underlying WS_FTP Server operating system. This vulnerability only affects customers who have the Ad Hoc module installed. This module is installed as part of a standard installation.

CVE-2023-42657 with a CVSS rating of 9.9, is a critical vulnerability that exists within WS_FTP Server versions prior to 8.7.4 and 8.8.2 and is a directory traversal vulnerability. 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.

Rapid7 has observed what appears to be exploitation of one or more of the WS_FTP vulnerabilities within their customers environments. Their reporting has confirmed that CVE-2023-40044 is exploitable with a single HTTPS POST request and the use of a pre-existing object deserialization tool.

Products Affected

Progress state that all versions of WS_FTP Server prior to 8.7.4 and 8.8.2 are affected by these vulnerabilities.

Impact

Exploitation of CVE-2023-40044 allows a pre-authenticated attacker to achieve Remote Code Execution (RCE) on the underlying WS_FTP Server operating system.

Exploitation of CVE-2023-42657 could allow an attacker 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.

Recommendations

All vulnerabilities listed in the Progress advisory have been addressed and the Progress WS_FTP team strongly recommends performing an upgrade to one of the fixed versions listed above.

They note that **"Upgrading to a patched release, using the full installer, is the only way to remediate this issue. There will be an outage to the system while the upgrade is running."**

For customers that are unable to patch immediately, Progress have released mitigation steps to disable the WS_FTP Server Ad Hoc Transfer Module.

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie