An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2610281061

NCSC Advisory

Critical Vulnerabilities in Progress Software: WS_FTP Server

CVE-2026-84295 and CVE-2026-90868

30th, October 2026

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.

Description

Published: 2026-10-29

Vendor: Progress Software

Product: WS_FTP Server

CVE ID: CVE-2026-84295 (**CVSS Score**[1]**:** 10)

CVE ID: CVE-2026-90868 (**CVSS Score**: 9.9)

Products Affected

CVE	Product	Version
CVE-2026-84295	WS_FTP Server	0 < 2024.0.6
CVE-2026-84295	WS_FTP Server	0 < 2025.0.3
CVE-2026-90868	WS_FTP Server	0 < 2024.0.7
CVE-2026-90868	WS_FTP Server	0 < 2025.0.4

Impact

CVE-2026-84295

Improper authentication in Progress Software WS_FTP Server versions prior to 2024.0.6 and 2025.0.3 on Windows could allow an unauthenticated remote attacker to access sensitive information, including administrative credentials.

Common Weakness Enumeration (CWE)[2]**:**

- CWE-287: Improper Authentication
- CWE-522: Insufficiently Protected Credentials

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE-2026-90868

An OS command injection vulnerability in Progress Software WS_FTP Server versions prior to 2024.0.7 and 2025.0.4 on Windows could allow arbitrary command execution under certain configurations.

Common Weakness Enumeration (CWE):

- CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
- CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Progress Software.

- https://nvd.nist.gov/vuln/detail/cve-2026-84295
- https://nvd.nist.gov/vuln/detail/CVE-2026-90868
- https://www.cve.org/CVERecord?id=CVE-2026-84295
- https://www.cve.org/CVERecord?id=CVE-2026-90868
- https://progress.lightning.force.com/lightning/r/Knowledge__kav/ka7P-b000001vl86IAA/view
- https://community.progress.com/s/article/WS-FTP-Server-Critical-Security-Alert-Bulletin-September-2026?popup=true&overview