National Cyber Security Centre

2311210130-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

CrushFTP Critical Vulnerability - CVE-2023-43177

Tuesday 21st November, 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.

Description

A critical vulnerability exists in CrushFTP which is being tracked as CVE-2023-43177. The vulnerability could allow an unauthenticated attacker to access files stored on the server, execute code remotely, or obtain plain text passwords.

A proof-of-concept (POC) exploit for CVE-2023-43177 has been publicly disclosed which is likely to be exploited by opportunistic actors. This makes it critical for CrushFTP users to install the security updates as soon as possible.

Products Affected

All CrushFTP versions **prior** to:

- 10.5.2

Impact

If exploited, it could allow an unauthenticated attacker to access all CrushFTP files, run arbitrary programs on the host server, and acquire plain-text passwords

To date, there have been no reports of the active exploitation of these vulnerabilities but future exploitation is deemed likely.

Recommendations

The NCSC strongly advises affected organisations to review the latest CrushFTP release notes and install the relevant update.

Apply these recommended steps, listed in order of priority to secure your CrushFTP servers:

- Update to the latest version of CrushFTP
- Set CrushFTP to the non-standard configuration of auto-update for new security patches when idle
- Audit for any unauthorised new user accounts and password changes via the user management dashboard and recent application logs
- Set CrushFTP to the non-standard configuration of auto-update for new security patches when idle
- The new hardened Limited Server mode, introduced by CrushFTP in response to Converge researcher feedback, should be enabled

Further information and additional measures to improve security can be found here:

- https://www.crushftp.com/version10.html
- https://convergetp.com/2023/11/16/crushftp-zero-day-cve-2023-43177-discovered/

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@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie