National Cyber Security Centre

2404240189-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in CrushFTP (CVE-2024-4040)

Wednesday 24th April, 2024

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: 2024-04-22T20:15:00
Vendor: CrushFTP
Product: CrushFTP
CVE ID: CVE-2024-4040
CVSS3.0 Score[1]**:** N/A
EPSS[2]**:** 0.094730000
(For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-4040)
Summary: A server side template injection vulnerability exists in **CrushFTP** in all versions before 10.7.1 and 11.1.0 on all platforms which allows unauthenticated remote attackers to read files from the filesystem outside of the VFS Sandbox, bypass authentication to gain administrative access, and perform remote code execution on the server.

Products Affected

- CrushFTP

Impact

Common Weakness Enumeration (CWE)[3]**:** CWE-1336 Improper Neutralization of Special Elements Used in a Template Engine

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO
Used by Ransomware Operators: Not Known

Recommendations

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

Additional recommendations and mitigation's for CVE-2024-4040 can be found in the respective links below:

- https://www.crushftp.com/crush10wiki/Wiki.jsp?page=Update
- https://www.reddit.com/r/cybersecurity/comments/1c850i2/all_versions_of_crush_ftp_are_vulnerable/
- https://www.bleepingcomputer.com/news/security/crushftp-warns-users-to-patch-exploited-zero-day-immediately/
- https://www.reddit.com/r/crowdstrike/comments/1c88788/situational_awareness_20240419_crushftp_virtual/
- https://www.rapid7.com/blog/post/2024/04/23/etr-unauthenticated-crushftp-zero-day-enables-complete-server-compromise/
- https://github.com/airbus-cert/CVE-2024-4040

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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