NCSC

National Cyber Security Centre

2401230277-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in Fortra GoAnywhere MFT (CVE-2024-0204)

Wednesday 24th January, 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

CVE Published: 2024-01-22T18:15:00
Vendor: Fortra
Product: GoAnywhere MFT
CVE ID: CVE-2024-0204
EPSS[1]**:** 0.240730000
Summary: Fortra has released an update to the file sharing platform GoAnywhere MFT. This update patches a vulnerability, CVE-2024-0204, which allows an unauthorised user to create an admin user via the administration portal. CVE-2024-0204 has a CVSS3.1 score of 9.8 (Critical).

More information related to this issue can be found at the following links:

- https://www.fortra.com/security/advisory/fi-2024-001
- https://my.goanywhere.com/webclient/ViewSecurityAdvisories.xhtml
- http://packetstormsecurity.com/files/176683/GoAnywhere-MFT-Authentication-Bypass.html

Products Affected

- Fortra GoAnywhere MFT 6.x from 6.0.1
- Fortra GoAnywhere MFT 7.x before 7.4.1

Impact

Successful exploitation of this vulnerability could allow an unauthorised user to create an administrator user.

At the time of writing, this vulnerability does not appear in the CISA Known Exploited Vulnerability (KEV)[2] catalog

Common Weakness Enumeration (CWE)[3]**:** CWE-425 Direct Request ('Forced Browsing')

Recommendations

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

Additional recommendations and mitigation's for the CVE can be found in the respective link(s) below: https://www.fortra.com/security/advisory/fi-2024-001

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

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