CYBER ADVISORY

TLP:CLEAR
23 January 2024

Fortra GoAnywhere MFT Vulnerability

CVE-2024-0204 | Fortra | Authentication Bypass | Critical Vulnerability

Executive Summary

The California Cyber Threat Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2024-0204.[1] The vulnerability affects Fortra's GoAnywhere MFT prior to version 7.4.1.[2] Exploitation of the vulnerability via authentication bypass could allow an attacker to create an admin user via the administration portal.[3,4]

The Cal-CSIC recommends immediately upgrade to version 7.4.1 or higher. The vulnerability may also be eliminated in non-container deployments by deleting the InitialAccountSetup.xhtml file in the install directory and restarting the services. For container-deployed instances, replace the file with an empty file and restart.

For further information on applying upgrades and mitigations, please refer to Fortra Security and Trust Center.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.

Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback here.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Bleeping Computer; "Fortra warns of new critical GoAnywhere MFT auth bypass, patch now;" https://www.bleepingcomputer.com/news/security/fortra-warns-of-new-critical-goanywhere-mft-auth-bypass-patch-now/; accessed 23 January 2024
[2] Github; "Authentication bypass in Fortra's GoAnywhere MFT prior to...;" https://github.com/advisories/GHSA-f8xf-39w2-mrc6; accessed 23 January 2024
[3] National Vulnerability Database; "CVE-2024-0204 Detail;" https://nvd.nist.gov/vuln/detail/CVE-2024-0204; accessed 23 January 2024
[4] Sec Alerts; "CVE-2024-0204: Authentication Bypass in GoAnywhere MFT;" https://secalerts.co/vulnerability/CVE-2024-0204; accessed 23 January 2024