NCSC
National Cyber Security Centre

2307130136-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability in customer-managed ShareFile storage zones CVE-2023-24489

Thursday 13th July, 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

Citrix have released a software update that addresses the vulnerability CVE-2023-24489 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24489. CVE-2023-24489 is a critical vulnerability in customer-managed ShareFile storage zones controllers which, if exploited, could allow unauthenticated arbitrary file upload and full remote code execution.

A Proof of Concept (PoC) has been made available online for this vulnerability.

Products Affected

This vulnerability affects all currently supported versions of customer-managed ShareFile storage zones controller before version 5.11.24.

Impact

Exploitation of CVE-2023-24489 could allow a remote attacker to perform unauthenticated arbitrary file uploads and full remote code execution.

Recommendations

The NCSC strongly advises all affected organisations of the Citrix ShareFile vulnerability to read the latest advisory from Citrix and apply available patches immediately:

https://support.citrix.com/article/CTX559517/sharefile-storagezones-controller-security-update-for-cve202324489

Information on upgrading storage zone controllers can be found here: https://docs.sharefile.com/en-us/storage-zones-controller/5-0/upgrade.html

Recent campaigns involving file transfer and storage solutions have highlighted the ease and speed with which malicious actors have leveraged vulnerabilities in similar products.

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