



**Computer Emergency Response Team of Mauritius**  
**Ministry of Information Technology, Communication and Innovation**

## **CERT-MU Vulnerability Note**

### **Citrix Vulnerabilities Actively Exploited by Hackers**

**Vulnerability Note:** VN-2025-20

**Date of Issue:** 26 August 2025

**Severity Rating:** High

**Systems Affected:**

- Citrix Session Recording
- Git

**Description**

Two critical Citrix Session Recording flaws and one Git vulnerability are being actively exploited and represent significant risks to organisations. The vulnerabilities identified are as follows:

- The first vulnerability (CVE-2024-8069) involves a deserialization of untrusted data vulnerability that allows attackers to execute malicious code by manipulating serialized data streams. This type of flaw has historically been favoured by threat actors due to its potential for remote code execution without authentication.
- The second Citrix vulnerability (CVE-2024-8068) centers on improper privilege management within the Session Recording component. This weakness enables attackers to escalate privileges and gain unauthorized access to sensitive system functions, potentially compromising entire network segments where Citrix infrastructure is deployed.
- The third vulnerability (CVE-2025-48384), affects Git version control systems through a link following weakness. This flaw could allow malicious actors to manipulate symbolic links, potentially leading to unauthorized file access or code repository compromise - a particularly concerning scenario for software development environments and source code management systems.

**CVE Information**

[CVE-2025-8069](#)

[CVE-2025-8068](#)

[CVE-2025-48384](#)

**Workaround**

- Organizations utilizing Citrix Session Recording solutions should immediately assess their exposure and implement available patches or mitigations.
- Similarly, environments running affected Git versions require prompt attention to prevent potential repository compromise.

**Postal address**

Mauritian Computer Emergency Response Team (CERT-MU)  
Ministry of Information Technology, Communication and Innovation  
2<sup>nd</sup> Floor, Wing A,  
Shri Atal Bihari Vajpayee Tower,  
Cybercity Ebene