

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

08/12/2020

**SUBJECT:**

Multiple Vulnerabilities in Citrix XenMobile Server Could Allow for Arbitrary File Read

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Citrix XenMobile Server, the most severe of which could allow for reading of arbitrary files on the server. XenMobile is a software that provides mobile device management and mobile application management. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary file read, resulting in access to configuration data and further attacks.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- XenMobile Server 10.12 before RP3
- XenMobile Server 10.11 before RP6
- XenMobile Server 10.10 before RP6
- XenMobile Server before 10.9 RP5

**RISK:**

**Government:**

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Citrix XenMobile Server, the most severe of which could allow for reading of arbitrary files on the server. Details of these vulnerabilities are as follows:

- A path traversal vulnerability that could allow reading of arbitrary files outside the web server root directory (CVE-2020-8209).
- One additional critical rated vulnerability (CVE-2020-8208).
- Multiple medium or low severity vulnerabilities (CVE-2020-8210, CVE-2020-8211, CVE-2020-8212)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary file read, resulting in access to configuration data and further attacks.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Citrix to vulnerable systems immediately after appropriate testing.
- Reset all password of logged in users over the past 120 days in case your organization was targeted by cyber threat actors.
- Apply the Principle of Least Privilege to all systems and services.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.

#### **REFERENCES:**

##### **CVE:**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8208>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8209>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8210>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8211>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8212>

##### **Citrix:**

<https://support.citrix.com/article/CTX277457>

##### **Positive Technologies:**

<https://www.ptsecurity.com/ww-en/about/news/citrix-fixes-xenmobile-vulnerability-found-by-positive-technologies/>

**TLP: WHITE**

**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**

<http://www.us-cert.gov/tlp/>