## Severity

High

## Analysis Summary

#### CVE-2021-44520 CVSS: 9.8

Citrix XenMobile Server could allow a remote attacker to execute arbitrary commands on the system, caused by a command injection flaw. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system.

#### CVE-2021-44519 CVSS: 9.8

Citrix XenMobile Server could allow a remote attacker to execute arbitrary commands on the system, caused by a command injection flaw. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system.

#### CVE-2022-26151 CVSS: 9.8

Citrix XenMobile Server could allow a remote attacker to execute arbitrary commands on the system, caused by a command injection flaw. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system.

#### CVE-2022-27503 CVSS: 6.1

Citrix StoreFront Server is vulnerable to cross-site scripting, caused by improper validation of user-supplied input when configured to use SAML authentication. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

#### CVE-2022-27506 CVSS: 4.9

Citrix SD-WAN could allow a remote authenticated attacker to gain unauthorized access to the system, caused by the use of hard-coded credentials. An attacker could exploit this vulnerability using the SD-WAN CLI to gain access to the shell.

#### CVE-2022-27505 CVSS: 6.1

Citrix SD-WAN is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

## Impact

- Code Execution
- Credential Theft
- Gain Access
- Unauthorized Access

## Indicator Of Compromise

#### CVE

- CVE-2021-44520
- CVE-2021-44519
- CVE-2022-26151
- CVE-2022-27503
- CVE-2022-27506

- CVE-2022-27505

## Affected Vendors

Citrix

## Affected Products

- Citrix XenMobile Server 10.13.0
- Citrix XenMobile Server 10.14.0
- Citrix StoreFront Server 1912 LTSR CU4 (1912.0.4000)
- Citrix StoreFront Server 3.12 for 7.15 LTSR CU8 (3.12.8000)
- Citrix SD-WAN 11.4.2 Standard
- Citrix SD-WAN 11.4.2 Premium
- Citrix SD-WAN Center Management Console 11.4.0
- Citrix SD-WAN Orchestrator for On-Premises 13.2.0
- Citrix SD-WAN 11.4.3 Standard
- Citrix SD-WAN 11.4.3 Premium

## Remediation

Please refer to the Citrix website for patches, updates, and workaround, visit:

Citrix XenMobile

Citrix StoreFront

Citrix SD-WAN