TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE 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:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
01/11/2022

SUBJECT:
A Vulnerability in Citrix Workspace App for Linux Could Allow for Local Privilege Escalation

OVERVIEW:
A vulnerability has been discovered in Citrix Workspace App for Linux, a virtual desktop application. Successful exploitation of this vulnerability could allow for local privilege escalation. A privilege escalation enables the attacker to obtain root privileges within the system which will enable them to install programs; view, change, or delete data; or create new accounts with full user rights.

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

SYSTEMS AFFECTED:
- Citrix Workspace App for Linux 2012 to 2111

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Citrix Workspace App for Linux, a virtual desktop application. This vulnerability has a pre-condition in that the Citrix Workspace App for Linux must be installed with App Protection. Successful exploitation of this vulnerability could allow for local privilege escalation. A privilege escalation enables the attacker to obtain root privileges within the system which will enable them to install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade Citrix Workspace App for Linux (2112 and later versions) to a fixed version as provided by Citrix.
- Verify no unauthorized changes have occurred before applying patches/updates.

REFERENCES:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21825

Citrix:
https://support.citrix.com/article/CTX338435

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE 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:WHITE information may be distributed without restriction.