CLOUD SECURITY CYBERATTACKS & DATA BREACHES THREAT INTELLIGENCE APPLICATION SECURITY

Citrix Patches Zero-Day Recording Manager Bugs

There is some disagreement over whether the remote code execution (RCE) security flaws allow for unauthenticated exploitation or not. Citrix says no, but researchers say the company is downplaying a "good old unauthenticated RCE."

Jai Vijayan, Contributing Writer
November 12, 2024

5 Min Read

SOURCE: JAVEPHOTO VIA SHUTTERSTOCK

Very swiftly after disclosing them, Citrix has issued patches for two vulnerabilities in its Citrix Virtual Apps and Desktop technology that allow a remote attacker escalate privileges or execute code of their choice on vulnerable systems.

Citrix has described the remote code execution (RCE) vulnerabilities as something that only a previously authenticated attacker could abuse. However, researchers at watchTowr who discovered the flaws and developed a proof-of-concept exploit (PoC) say it's a point-and-click vulnerability that an unauthenticated attacker can exploit with relative ease.

Citrix is tracking one of the flaws as CVE-2024-8068 and the other as CVE-2024-8069. A few hours after Citrix and watchTowr made their announcements, the ShadowServer Foundation announced it was seeing PoC-based exploitation attempts.

"While there is discussion on whether these are remotely exploitable without auth, we urge you to update your installations NOW," it write in an email.

Citrix Downplaying Threat Severity?

The flaws affect the thin-client technology's Session Recording Manager component that allows admins to capture, store, and manage recordings of user sessions. They stem from a weakness in how Session Recording Manager deserializes or unpacks data that has been converted into a format that makes it easy to store and transmit, according to the researchers at watchTowr who discovered and reported the issues to Citrix in July.

Related: Thrive Acquires Secured Network Services

Citrix initially said it was unable to reproduce the issue but later acknowledged the problem after the security vendor gave them a PoC exploit for the vulnerability.

In an advisory issued Nov. 12, the company described CVE-2024-8068 as a privilege escalation vulnerability that allows an authenticated user in the same Windows Active Directory domain as the session recording server to gain NetworkService Account access. CVE-2024-8069, according to Citrix, is a "limited" RCE for attackers with admin-level account access on vulnerable systems. "Cloud Software Group strongly urges affected customers of Citrix Session Recording to install the relevant updated versions of Citrix Session Recording as soon their upgrade schedule permits," the company cautioned.

Don't miss the upcoming free Dark Reading Virtual Event, "Know Your Enemy: Understanding Cybercriminals and Nation-State Threat Actors," Nov. 14 at 11a.m. ET. *Don't miss sessions on understanding MITRE ATT&CK; using proactive security as a weapon, and a masterclass in incident response; and a host of top speakers like Larry Larsen from the Navy Credit Federal Union, former Kaspersky Lab analyst Costin Raiu, Ben Read of Mandiant Intelligence, Rob Lee from SANS, and Elvia Finalle from Omdia.* ***Register now!***

Related: Databarracks Launches Air Gap Recover

Even so, Citrix has assigned both vulnerabilities only medium severity scores of 5.1 of 10 on the CVSS vulnerability rating scale. It's an assignment that watchTowr has disputed.

"Citrix is downplaying the severity of this vulnerability as a medium priority when it's really point-click-full-takeover," says Benjamin Harris, CEO of watchTowr, pointing to the company's exploit code. The combination of the two vulnerabilities allows for a "good old unauthenticated RCE," Harris tells Dark Reading.

"Citrix's Virtual Apps and Desktop offering is a flagship Citrix solution, targeted at [Fortune 500] organizations," he notes. "Since we're dealing with a deserialization issue, a bug class that is known for being relatively stable, we [have] a high degree of confidence that our exploit will work reliably. There's no tricky heap manipulation or other entropy creeping in."

Many organizations use Citrix's Virtual Apps and Desktop technology to enable users to access their applications and desktop environments from anywhere and using any device. It gives organizations a way to centrally deploy, update, and secure all user apps from a single location making maintenance more efficient, consistent, and cost effective. Another benefit that Citrix advertises is increased security from having applications and data on centralized servers rather than on individual endpoint devices. The technology's Session Recording feature — where watchTower discovered the flaws — enables admins to monitor for anomalous behavior and to maintain a detailed record of user activity for future audit and troubleshooting purposes.

Related: Chinese 'Infrastructure Laundering' Abuses AWS, Microsoft Cloud

Demand for such technologies has increased in recent years as more companies have embraced remote and hybrid work models. Research firm MarketsandMarkets estimates the market will reach $1.7 billion in 2028 from around $1.5 billion last year. The broader desktop-as-a-service (DaaS) market itself is expected to hit nearly $19 billion by 2030 from just over $4 billion in 2021.

Dependence on Known Insecure Technology

The researchers at watchTower discovered the vulnerabilities while scrutinizing Citrix's Virtual Apps and Desktop's architecture for potential security issues. The security vendor's examination showed that Citrix's app uses Microsoft's Message Queuing (MSMQ) service to receive recorded user session files and to store them in a separate storage manager component. In addition, watchTower found Citrix using a Microsoft technology called BinaryFormatter to deserialize data in the storage manager component when needed. BinaryFormatter is technology that Microsoft itself has urged organizations to stop using as soon as possible because of security weaknesses that are no longer fixable, watchTower said.

The vulnerabilities that watchTower discovered involved a combination of an Internet-accessible MSMQ instance in the session recording component of Citrix's Virtual Apps and Desktop technology along with misconfigured permissions related to BinaryFormatter. "This isn't really a bug in the BinaryFormatter itself, nor a bug in MSMQ, but rather the unfortunate consequence of Citrix relying on the documented-to-be-insecure BinaryFormatter to maintain a security boundary," Harris says. "It's a 'bug' that manifested during the design phase, when Citrix decided which serialization library to use."

Harris says watchTower reported the vulnerability as a single issue, whereas Citrix appears to have treated it as two separate issues.

"While it is inarguable that Citrix's use of a BinaryFormatter with untrusted data is a de facto bug," Harris says, "we don't have enough context to determine if exposing the MSMQ queue via HTTP is really a bug, caused by a careless oversight, or a carefully calculated effect of some obscure business requirement."

Citrix's technologies are a frequent target for attackers because of the high level of access the company's technology provides to enterprise applications and data. Many of the reported security flaws recently have affected the company's NetScaler ADC and NetScaler Gateway remote access platforms.

About the Author

Jai Vijayan, Contributing Writer

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security...

You May Also Like

Thousands of ServiceNow KB Instances Expose Sensitive Corporate...

Socially Savvy Scattered Spider Traps Cloud Admins in Web

Cyberattackers Accessed HealthEquity Customer Info via Third Party

Multifactor Authentication Is Not Enough to Protect Cloud Data

More Insights

Webinars

Securing the Remote Workforce
FEB 20, 2025

Emerging Technologies and Their Impact on CISO Strategies
FEB 25, 2025

How CISOs Navigate the Regulatory and Compliance Maze
FEB 26, 2025

Where Does Outsourcing Make Sense for Your Organization?
FEB 27, 2025

Shift Left: Integrating Security into the Software Development Lifecycle
MAR 5, 2025

More Webinars

Events

[Conference] Black Hat USA - August 2-7 - Learn More

[Conference] Black Hat Asia - April 1-4 - Learn More

[Dark Reading Virtual Event] Cybersecurity's Most Promising New and Emerging Technologies

More Events

Editor's Choice

Microsoft's February Patch a Lighter Lift Than January's

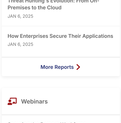
by Jai Vijayan, Contributing Writer

FEB 11, 2025 4 MIN READ

DeepSeek AI Fails Multiple Security Tests, Raising Red Flag for Businesses

by Elizabeth Montalbano, Contributing Writer

FEB 11, 2025 4 MIN READ



Salt Typhoon's Impact on the US & Beyond

by Michael McLaughlin, Jillian Cash and 1 more

FEB 11, 2025 4 MIN READ

Reports

The State of Firewall Security: Challenges, Risks, and Solutions for Modern Networks
JAN 10, 2025

Industrial Networks in the Age of Digitalization
JAN 6, 2025

Zero-Trust Adoption Driven by Data Protection, Cloud Access Control, and Regulatory Compliance Requirements
JAN 6, 2025

Threat Hunting's Evolution: From On-Premises to the Cloud
JAN 6, 2025

How Enterprises Secure Their Applications
JAN 6, 2025

More Reports

Webinars

Securing the Remote Workforce
FEB 20, 2025

Emerging Technologies and Their Impact on CISO Strategies
FEB 25, 2025

How CISOs Navigate the Regulatory and Compliance Maze
FEB 26, 2025

Where Does Outsourcing Make Sense for Your Organization?
FEB 27, 2025

Shift Left: Integrating Security into the Software Development Lifecycle
MAR 5, 2025

More Webinars

White Papers

6 Key Requirements of Multicloud Security

Delivering Globally Consistent App Performance to the Hybrid Workforce

Secure remote access. Simplified.

4 Best Practices for Hybrid Security Policy Management

The State of Asset Security: Uncovering Alarming Gaps & Unexpected Exposures

More Whitepapers

Events

[Conference] Black Hat USA - August 2-7 - Learn More
AUG 2, 2025

[Conference] Black Hat Asia - April 1-4 - Learn More
APR 1, 2025

[Dark Reading Virtual Event] Cybersecurity's Most Promising New and Emerging Technologies
MAR 20, 2025

More Events