

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



## VMware Patches Critical Flaw in Workspace ONE UEM Console

By [Ionut Arghire](#) on December 17, 2021

Share

Tweet

推荐 6



VMware on Thursday announced the release of patches for a critical server-side request forgery (SSRF) vulnerability in Workspace ONE UEM console.

An attacker could exploit the flaw to access sensitive data in the management console, VMware says. Tracked as [CVE-2021-22054](#), the security error carries a CVSS score of 9.1.

To exploit the vulnerability, an attacker needs to have network access to UEM, so they can send unauthenticated requests and trigger the bug.

The vulnerability was reported privately to the cloud computing and virtualization technology company, and both patches and workarounds have been released to address it.

CVE-2021-22054 was fixed with the release of VMware Workspace ONE UEM console versions 21.5.0.37, 21.2.0.27, 20.11.0.40, and 20.0.8.36. VMware Workspace ONE UEM patch 21.9.0.13 and above also address the bug.

VMware also says it has mitigated the issue for VMware-hosted Workspace ONE consoles and notes that some workarounds are available for on-premises installations.

“The issue has been mitigated across all SaaS environments through infrastructure changes which will remain in place until VMware Cloud Operations has deployed the necessary patches,” VMware says.

Organizations that cannot patch their on-premises environments can find available workarounds in a [support article](#). The workaround was designed to block access to a specific endpoint when the request includes a 'url' query parameter, thus removing the possibility of exploitation.

Related: [VMware Patches File Read, SSRF Vulnerabilities in vCenter Server](#)

Related: [VMware Working on Patches for Serious vCenter Server Vulnerability](#)

Related: [VMware Calls Attention to High-Severity vCenter Server Flaw](#)

Share

Tweet

推荐 6

RSS



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Trend Micro Spots Chinese Hackers Targeting Transportation Sector](#)

[Phorpiex Botnet Hijacked 3,000 Cryptocurrency Transactions](#)

[VMware Patches Critical Flaw in Workspace ONE UEM Console](#)

[Sophisticated Noberus Ransomware First to Be Coded in Rust](#)

[Iran-Linked APT Abuses Slack in Attacks on Asian Airline](#)

[2021 Singapore/APAC ICS Cyber Security Conference \[Virtual: June 22-24\]](#)

sponsored links

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

[2021 ICS Cyber Security Conference | USA \[Hybrid: Oct. 25-28\]](#)

[2021 CISO Forum: September 21-22 - A Virtual Event](#)

Tags:

[NEWS & INDUSTRY](#) [Vulnerabilities](#)

Search

**Get the Daily Briefing**

**BRIEFING**

Business Email Address

Subscribe

