VMware vCenter Server Updates Address Critical Vulnerabilities

Overview

VMware has released updates addressing two vulnerabilities in VMware vCenter Server and VMware Cloud Foundation. These include a heap-overflow vulnerability (CVE-2024-38812) and a privilege escalation vulnerability (CVE-2024-38813). Exploitation of these vulnerabilities has been observed in the wild.

CVE-2024-38812 (CVSS 9.8) is a heap-overflow vulnerability in the DCERPC protocol implementation. The vulnerability could allow for remote code execution via specially crafted network packets. Exploitation of CVE-2024-38812 could lead to full system compromise of VMware vCenter Server. This could result in unauthorized access and data breaches.

CVE-2024-38813 (CVSS 7.5) is a privilege escalation vulnerability that could give attackers root-level privilege escalation through network packet manipulation. Exploitation of CVE-2024-38813 could give attackers complete control over affected VMware vCenter Server systems. This could lead to unauthorized configuration changes, deployment of malicious payloads, or further compromise of connected systems and sensitive data.

Affected Products:

- VMware vCenter Server 7.0, 8.0
- VMware Cloud Foundation 4.x, 5.x

Aspire recommends patching these vulnerabilities as soon as possible.

Aspire Protects

- **Patch –** Apply VMware's patches as soon as possible. You may find patch guidance in VMware's advisory.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Targeting vCenter DCERPC with malicious packets.

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548.002) – Exploiting privilege escalation vulnerabilities to gain root access.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

- The targeted industries for these vulnerabilities are likely those heavily reliant on VMware vCenter Server and Cloud Foundation, including:
    - Technology and IT Services - Organizations managing virtualized environments.
    - Financial Services - Due to their extensive use of virtualized infrastructure for scalability and security.
    - Healthcare - With a reliance on virtualized systems for patient data and operations.
    - Government and Defense - Hosting critical systems in virtualized environments.
    - Retail and E-commerce - Managing digital platforms and inventory systems on virtual servers.

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
    - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Support Content Notification - Support Portal - Broadcom support portal