THREAT ADVISORY

June 26, 2023

Multiple Vulnerabilities in VMware Products Could Allow for Arbitrary Code Execution

OVERVIEW

Multiple vulnerabilities have been discovered in VMware vCenter Server and Cloud Foundation, the most severe of which could allow for arbitrary code execution. VMware vCenter Server is the centralized management utility for VMware. VMware Cloud Foundation is a multi-cloud platform that provides a full-stack hyperconverged infrastructure (HCI) that is made for modernizing data centers and deploying modern container-based applications. Successful exploitation of these vulnerabilities could allow for arbitrary code execution in the context of the administrator account. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE

There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED

- VMware - VMware vCenter Server (vCenter Server) versions prior to 8.0 U1b
- VMware - VMware vCenter Server (vCenter Server) versions prior to 7.0 u3m
- VMware - VMware Cloud Foundation (vCenter Server) versions prior to 7.0 U3m, 8.0 U1b

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

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

Homes: Low

TECHNICAL SUMMARY

Multiple vulnerabilities have been discovered in VMware vCenter Server and Cloud Foundation, most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

Tactic: *Initial Access* (TA0001):

Technique: *Exploit Public-Facing Application (T1190):*

- CVE-2023-20892 - VMware vCenter Server heap-overflow vulnerability - The vCenter Server contains a heap overflow vulnerability due to the usage of uninitialized memory in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may exploit heap-overflow vulnerability to execute arbitrary code on the underlying operating system that hosts vCenter Server.

- CVE-2023-20893 - VMware vCenter Server use-after-free vulnerability - The VMware vCenter Server contains a use-after-free vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may exploit this issue to execute arbitrary code on the underlying operating system that hosts vCenter Server.

Details of lower-severity vulnerability are as follows:

- CVE-2023-20894 - The VMware vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bound write by sending a specially crafted packet leading to memory corruption.

- CVE-2023-20895 - The VMware vCenter Server contains a memory corruption vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger a memory corruption vulnerability which may bypass authentication.

- CVE-2023-20896 - The VMware vCenter Server contains an out-of-bounds read vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds read by sending a specially crafted packet leading to denial-of-service of certain services (vmcad, vmdird, and vmafdd).

Successful exploitation of these vulnerabilities could allow for arbitrary code execution in the context of the administrator account. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
|

RECOMMENDATIONS
We recommend the following actions be taken:

- Apply appropriate updates provided by VMware to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)

    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

    - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.

    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)

- **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.

- **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc. (**M1035: Limit Access to Resource Over Network**)

- Use intrusion detection signatures to block traffic at network boundaries. (**M1031: Network Intrusion Prevention**)

    - **Safeguard 13.3: Deploy a Network Intrusion Detection Solution:** Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

    - **Safeguard 13.8: Deploy a Network Intrusion Prevention Solution:** Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)

Safeguard 13.10: Performing Application Layer Filtering: Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.

REFERENCES

- https://www.vmware.com/security/advisories/VMSA-2023-0014.html
- https://kb.vmware.com/s/article/88287
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20892
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20893
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20894
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20895
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20896