Detect a critical flaw in VMware Cloud Director, which could pave the way for hackers to take control of enterprise servers

The newly discovered vulnerability in VMware's Cloud Director platform has the ability to allow attackers to access sensitive information and even control private clouds throughout the infrastructure.

On June 1, security researchers from cybersecurity firm Citadelo (Czech Republic) revealed details about a newly discovered vulnerability in VMware's Cloud Director platform that could potentially enable allow an attacker to access sensitive information and even control private clouds throughout the infrastructure. Citadelo stumbled upon the flaw while conducting a secure cloud infrastructure audit of an anonymous large enterprise (on the Fortune 500 list).

Cloud Director

With these characteristics, it is not too difficult to understand when this vulnerability receives a score of 8.8 / 10 on the CVSS v.3 - classified as 'Critical' and is currently being monitored internationally. with identifier CVE-2020-3956.

According to the initial conclusion, this is a code injection flaw that originates from a certain flaw that appears in the process of processing input data of Cloud Director. Hackers can take full advantage of this vulnerability to send malicious network traffic to Cloud Director, allowing them to execute arbitrary code on the victim's system.

Basically, VMware Cloud Director is a software that supports management, automation and deployment used relatively popular in the global business community. Provides solutions to operate and manage cloud resources,

allowing businesses to establish secure connections to different data centers and turn them into virtual data centers.

CVE-2020-3956 can be exploited through HTML5 and Flex-based UIs, API Explorer Interface, and API Access, as well as directly affect VMware Cloud Director 10.0.x versions (prior to 10.0.0.2) ; VMware Cloud Director 9.7.0.x (before 9.7.0.5); VMware Cloud Director 9.5.0.x (before 9.5.0.6) and VMware Cloud Director 9.1.0.x (before 9.1.0.4).

Successfully exploiting the vulnerability, hackers can perform the following malicious activities:

1. View the contents of the internal system database, including the passwords of any customers allocated to this infrastructure.
2. Modify the system database to access virtual machines (VMs) assigned to different organizations in Cloud Director.
3. Enhance privileges from "Organization Administrator" to "System Administrator ', along with access to all cloud accounts just by changing the password via SQL query.
4. Modify the login page of Cloud Director, allowing an attacker to gain the password of a customer, including the System Administrator account.
5. Read other sensitive customer-related data, such as full name, email address or IP address.

VMware has now released the corresponding patches for the Cloud Director versions affected by the vulnerability. If your company is using Cloud Director, quickly update to the latest version.