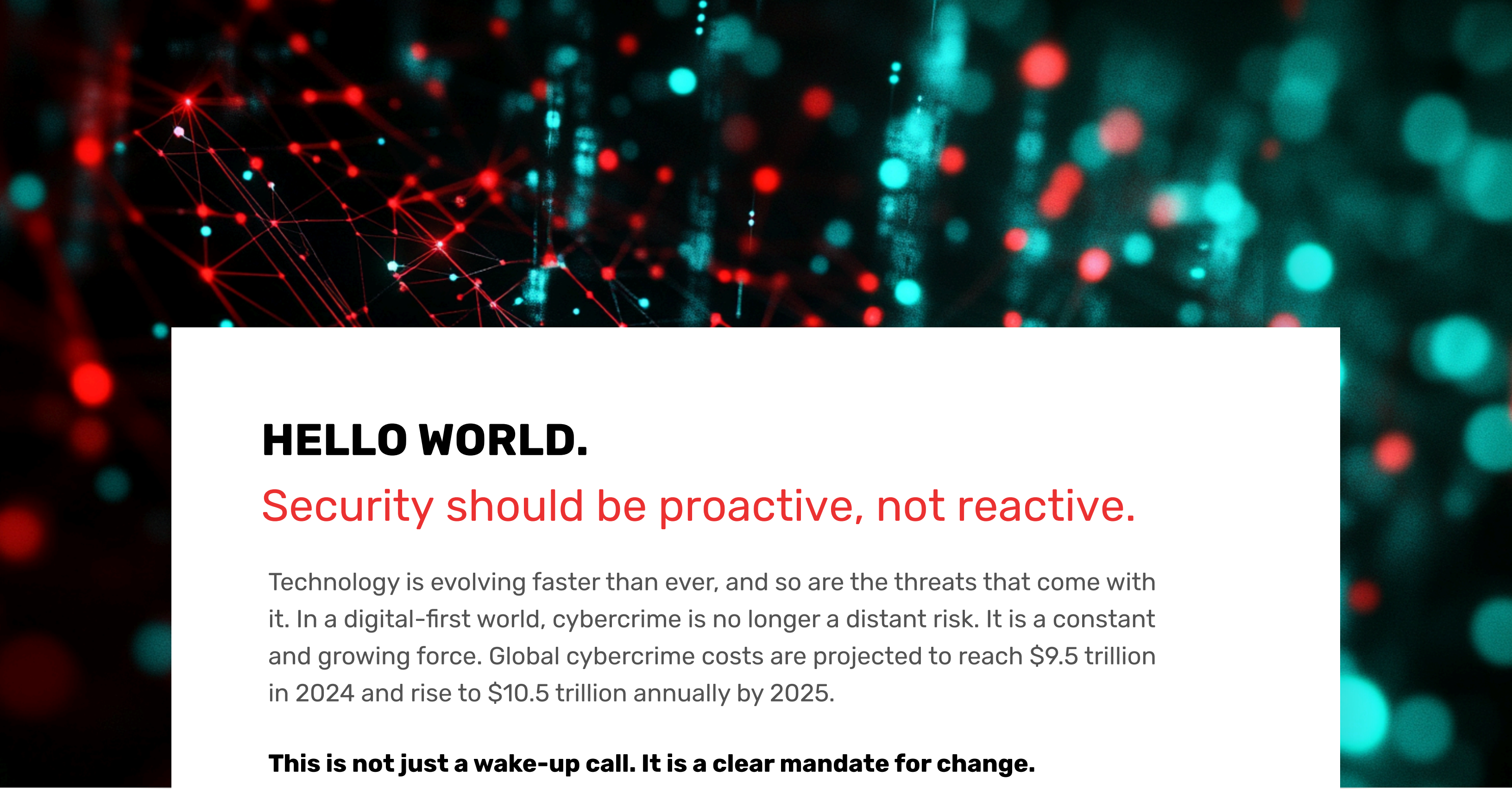
VONAHI SECURITY
A Kaseya COMPANY

2025 REPORT

Top 10 Critical Pentest Findings



HELLO WORLD.

Security should be proactive, not reactive.

Technology is evolving faster than ever, and so are the threats that come with it. In a digital-first world, cybercrime is no longer a distant risk. It is a constant and growing force. Global cybercrime costs are projected to reach $9.5 trillion in 2024 and rise to $10.5 trillion annually by 2025.

This is not just a wake-up call. It is a clear mandate for change.
Today's IT and security leaders must go beyond basic checkboxes. Compliance and cyber insurance now demand proof that defenses are working against real-world threats. Unfortunately, traditional network penetration testing often falls short. It is expensive, slow, and usually performed only once a year, leaving long periods where vulnerabilities go unchecked.

At Vonahi Security, we offer a better solution.
vPenTest is an automated network penetration testing platform that delivers proactive, on-demand assessments. It replicates real attacker behavior to identify true risks in real time, without requiring additional staff or outsourcing. This modern approach enables more frequent, scalable, and cost-effective testing, giving organizations consistent visibility into their security posture throughout the year. Because in today's cybersecurity landscape, once a year is no longer enough.

After running over **50,000** automated network penetration tests in 2024, Vonahi Security identified the **Top 10 Critical Internal Pentest Findings** across 20,000+ organizations. This resource helps security teams stay informed and one step ahead of the bad guys.

Alton Johnson
Founder & Principal Security Consultant
Vonahi Security

Table of Contents

OVERVIEW

Vonahi Security has provided over 20,000 organizations with a full-scale automated network penetration test since 2019 through our SaaS platform. This report shows the top 10 critical internal network pentest findings based on the 9,000+ security tests performed globally, as delivered by our vPenTest platform last year in 2024.

TOP 10 CRITICAL INTERNAL PENTEST FINDINGS BASED ON % OF OCCURRENCE

66.0 %	Multicast DNS (mDNS) Spoofing
61.6 %	NetBIOS Name Service (NBNS) Spoofing
57.0 %	Link-Local Multicast Name Resolution (LLMNR) Spoofing
47.2 %	IPv6 DNS Spoofing
21.8 %	Outdated Microsoft Windows Systems
12.6 %	IPMI Authentication Bypass
4.1 %	Microsoft Windows RCE (EternalBlue)
3.8 %	Microsoft Windows RCE (BlueKeep)
1.4 %	Firebird Servers Accept Default Credentials
1.2 %	Active Directory Certificate Services Privilege Escalation Vulnerabilities

TOP 10 CRITICAL INTERNAL PENTEST FINDINGS BY INDUSTRIES

11.5%	Healthcare
11.4%	Technology
9.4%	Banking/Finance
7.8%	Manufacturing
5.6%	IT Services
4.5%	Legal
3.9%	Construction
3.3%	Government
3.1%	Education
3.0%	Non-Profit

DEFINITIONS

PENTEST FINDINGS

The vulnerabilities that were successfully exploited by our automated pentesting platform, vPenTest, while performing an assessment in a non-disruptive manner on internal and external networks. PenTest findings will be referred to as “Findings” throughout the report.

THREAT SEVERITY RANKING

To assist organizations with prioritizing findings, the pentest findings and observations are categorized with threat severity rankings based on the Common Vulnerability Scoring System. The CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. CVSS is currently at version 3.1.

Severity	Description
Critical CVSS 9.0-10.0	A critical threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but pose a significant threat to the confidentiality, integrity, and/or availability of the organization’s systems and data. A successful compromise of findings of this ranking lead to access to multiple systems and/or several pieces of sensitive information.
High CVSS 7.0-8.9	A high threat ranking requires immediate remediation or mitigation. Exploitation of these vulnerabilities typically require a minimal amount of effort by the adversary, but pose a significant threat to the confidentiality, integrity, or availability of the organization’s systems or data. A successful compromise of findings of this ranking lead to access to a single access or limited sensitive information.
Medium CVSS 4.0-6.9	A medium threat ranking requires remediation or mitigation within a short and reasonable amount of time. These findings typically lead to a compromise of non-privileged user accounts on systems and/or applications or denote a denial-of-service (DoS) condition of the host, service, or application.
Low CVSS 0.1-3.9	A low threat ranking requires remediation or mitigation once all higher prioritized findings have been remediated. These findings typically leak information to unauthorized or anonymous users and may lead to more significant attacks when combined with other attack vectors.
Informational CVSS 0	An information threat ranking does not pose a significant threat to the environment and may just be findings that could potentially disclose valuable information, but does not expose the organization to any technical attacks. Findings rated as informational may be useful for an attacker performing information gathering on the organization to leverage in other attacks, such as social engineering or phishing.

Frequency of occurrence: 66%

01 MULTICAST DNS (mDNS) SPOOFING

Multicast DNS (mDNS) serves as a name resolution protocol for local networks, facilitating the resolution of domain names when a dedicated DNS server is unavailable. The resolution process occurs in stages:

1. The system first consults its local host file for any appropriate DNS name/IP address mappings.
2. In the absence of a configured DNS server, the system resorts to mDNS, broadcasting an IP multicast query requesting identification from the host corresponding to the DNS name. This protocol behavior exposes a potential vulnerability that malicious actors can exploit, enabling them to impersonate legitimate systems by responding to these queries.

RECOMMENDATIONS

- To mitigate the risk of mDNS spoofing, the primary recommendation is to completely disable mDNS if it is not in use. On Windows systems, this can often be done by implementing the 'Disable Multicast Name Resolution' group policy. As many applications have the potential to reintroduce mDNS functionality, an alternative strategy is to block UDP port 5353 via the Windows firewall. For non-Windows systems, disabling services such as Apple Bonjour or avahi-daemon can provide similar protection.
- It is important to note that disabling mDNS may disrupt functionalities such as screen casting and certain conference room technologies. Should complete disabling not be feasible, consider isolating affected systems within a controlled network segment and mandating the use of strong, complex passwords for any accounts that access these systems.

REPRODUCTION STEPS

On a system configured with mDNS, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the mDNS traffic on the internal network environment by filtering for UDP queries over port 5353.

SECURITY IMPACT

CVSS3.1

9.8

mDNS queries, which are transmitted across the local subnet, can be answered by any device capable of receiving them. This vulnerability allows an attacker to respond with their system's IP address, potentially misleading the querying system. Such exploitation may lead to interception of sensitive info, including unencrypted and hashed credentials, depending on the specific service the victim is trying to access (e.g., SMB, HTTP, MSSQL). It should be noted that hashed credentials can often be compromised within a relatively short timeframe using modern computing resources and brute-force attack methodologies.

REFERENCES

Multicast DNS

Frequency of occurrence: 61.6%

02 NETBIOS NAME SERVICE (NBNS) SPOOFING

The NetBIOS Name Service (NBNS) is a protocol utilized by workstations within an internal network to resolve domain names when a DNS server is unavailable or unresponsive. When a system attempts to resolve a DNS name, it follows these steps:

1. The system first checks its local host file for an entry mapping the DNS name to an IP address.
2. If no local mapping exists, the system sends a DNS query to its configured DNS server(s) in an attempt to retrieve the corresponding IP address.
3. If the DNS server(s) cannot resolve the name, the system broadcasts an NBNS query across the local network, soliciting responses from other systems.

This dependency on broadcasts makes the NBNS vulnerable to spoofing attacks, wherein an attacker can respond with a false IP address.

RECOMMENDATIONS

- To mitigate the risk of NBNS spoofing, it is advisable to disable the NetBIOS service across all hosts within the internal network. This can be accomplished through a variety of methods including configuration of DHCP options, adjustments to network adapter settings, or modifications to the system registry. Implementing these changes will significantly reduce the potential attack surface associated with NBNS.

REPRODUCTION STEPS

On a system configured with NBNS, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the broadcasted traffic on the internal network environment.

SECURITY IMPACT

CVSS3.1

9.8

The broadcasting nature of NBNS queries means that any system on the local network can respond. This vulnerability can be exploited by malicious actors who may answer these queries with the IP address of the attacker's system, redirecting traffic intended for legitimate services. For instance, services such as SMB, MSSQL, or HTTP could inadvertently send sensitive data, including cleartext or hashed account credentials, to the attacker's system. Moreover, modern computational capabilities can facilitate the cracking of hashed credentials, potentially allowing unauthorized access to user accounts.

REFERENCES

NTLM Challenge Response is 100% Broken

How to disable NetBIOS over TCP/IP by using DHCP server options

Disabling NetBIOS over TCP/IP Via Registry

NetBIOS over TCP/IP Configuration Parameters

Frequency of occurrence: 57%

03 LINK-LOCAL MULTICAST NAME RESOLUTION (LLMNR) SPOOFING

Link-Local Multicast Name Resolution (LLMNR) is a protocol used amongst workstations within an internal network environment to resolve a domain name system (DNS) name when a DNS server does not exist or cannot be helpful.

When a system attempts to resolve a DNS name, it proceeds with the following steps:

1. The system checks its local host file to determine if an entry exists to match the DNS name in question with an IP address.
2. If the system doesn't have an entry in its local hosts file, the system then sends a DNS query to its configured DNS server(s) to attempt retrieving an IP address that matches the DNS name in question.
3. If the configured DNS server(s) cannot resolve the DNS name to an IP address, the system then sends an LLMNR broadcast packet on the local network to seek assistance from other systems.

RECOMMENDATIONS

To mitigate the risks associated with LLMNR spoofing, it is critical to disable LLMNR functionality across affected systems. This can be accomplished through the following methods:

- **Group Policy Configuration:** Navigate to Computer Configuration\Administrative Templates\Network\DNS Client and set 'Turn off Multicast Name Resolution' to Enabled. For administering configurations on a Windows Server 2003 domain controller, utilize the Remote Server Administration Tools for Windows 7 available at this link.
- **Registry Modification for Windows Vista/7/10 Home Edition:** Access the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient and modify the 'EnableMulticast' key to 0 or remove it to disable the feature.

REPRODUCTION STEPS

On a system configured with LLMNR, attempt to interact with a DNS name that is known to be invalid (e.g. test123.local). On another system, use a network packet analyzer, such as Wireshark, to inspect the broadcasted traffic on the internal network environment.

SECURITY IMPACT

CVSS3.1

9.8

Since the LLMNR queries are broadcasted across the network, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using modern-day computing power and brute-force techniques.

REFERENCES

Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay

Remote Server Administration Tools (RSAT) for Windows

Frequency of occurrence: 47.2%

04 IPV6 DNS SPOOFING

The risk of IPv6 DNS spoofing arises from the possible introduction of a rogue DHCPv6 server within the internal network infrastructure. Due to the preference of Microsoft Windows systems for IPv6 over IPv4, IPv6-capable clients are inclined to obtain their IP address configurations from any available DHCPv6 server.

RECOMMENDATIONS

To mitigate the risks associated with IPv6 DNS spoofing, the following strategies are recommended, with emphasis on aligning each approach with organizational operations and thorough testing prior to implementation:

- **Manage Rogue DHCP at the Network Layer:** Implement features such as Rogue DHCP detection, DHCP snooping, and DHCP authentication on network switches and firewalls to control unauthorized DHCP servers and lessen the likelihood of DNS spoofing attacks.
- **Prefer IPv4 over IPv6:** Utilize Group Policy Objects (GPOs) or Group Policy Preferences (GPPs) to deploy registry modifications that configure Windows systems to favor IPv4 over IPv6. It is important to note that this approach will not prevent attacks from affecting non-Windows devices.
- **Disable IPv6:** While not generally advisable for Microsoft Windows systems, disabling IPv6 may be considered as a last resort precaution, provided thorough testing ensures there are no significant disruptions to business operations.

REPRODUCTION STEPS

Leveraging the "mitm6" tool within Kali Linux, a user is able to quickly deploy a DHCPv6 server within the local network and assign five-minute leases (by default) to IPv6-enabled clients.

SECURITY IMPACT

CVSS3.1

10.0

The deployment of a rogue DHCPv6 server allows an attacker to manipulate DNS requests by redirecting IPv6-enabled clients to utilize the attacker's system as their DNS server. This capability can lead to serious consequences, such as the unauthorized capture of sensitive data, including user credentials. When all DNS queries resolve to the attacker's server, the victim's system may inadvertently communicate with malicious services operating on the attacker's infrastructure, encompassing platforms such as SMB, HTTP, RDP, and MSSQL.

REFERENCES

Taking Over IPv6 Networks

Guidance for configuring IPv6 in Windows for advanced users

Frequency of occurrence: 21.8%

05 OUTDATED MICROSOFT WINDOWS SYSTEMS

Outdated Microsoft Windows system(s) present significant security risks, as they are no longer receiving critical updates from Microsoft. These system(s) may lack essential security patches addressing known vulnerabilities, effectively rendering them more susceptible to exploitation by attackers. Additionally, the absence of updates can result in compatibility issues with modern security tools and software, further diminishing the system(s)' defenses. Vulnerabilities on outdated systems can often be exploited in attacks, such as malware distribution, data exfiltration, and unauthorized access.

RECOMMENDATIONS

It is strongly recommended to replace outdated versions of Microsoft Windows with current operating system(s) that are still supported by the manufacturer. This should include conducting a thorough inventory of all system(s) to identify and prioritize outdated versions, followed by implementing a phased upgrade strategy. Regularly verify that all system(s) are receiving the latest updates and patches to maintain security integrity.

REPRODUCTION STEPS

Use an operating system identification scanner, such as Nmap or Metasploit, to scan the affected targets to identify their specific versions. Alternatively, a network administrator can check the operating system version by logging into the system and viewing the operating system version through the system properties.

SECURITY IMPACT

CVSS3.1

9.8

If exploited, an outdated Microsoft Windows system could allow an attacker to gain unauthorized access to the affected system(s), exposing sensitive data and resources. Furthermore, due to the potential similarity in configurations among system(s) within the same network, an attacker may utilize the compromised system(s) as a launching point to move laterally, compromising additional system(s) and increasing the overall footprint of the breach.

REFERENCES

Mitre ATT&CK Mitigations - Update Software

What does it mean if Windows isn't supported?

Frequency of occurrence: 12.6%

06 IPMI AUTHENTICATION BYPASS

The Intelligent Platform Management Interface (IPMI) is a critical hardware solution utilized by network administrators for centralized management of server(s). During the configuration of server(s) equipped with IPMI, certain vulnerabilities may exist that allow attackers to bypass the authentication mechanism remotely. This results in the extraction of password hashes, and in instances where default or weak hashing algorithms are employed, attackers could potentially recover the cleartext passwords.

RECOMMENDATIONS

Given the absence of a patch for this vulnerability, it is essential to implement one or more of the following mitigation strategies:

- Limit IPMI access strictly to authorized system(s) that require administrative functionalities.
- Disable IPMI service on server(s) that do not need it for business operations.
- Change default administrator password(s) to strong, complex alternatives to enhance security.
- Employ secure communication protocols, such as HTTPS and SSH, to mitigate the risk of man-in-the-middle attacks that could expose sensitive credentials.

REPRODUCTION STEPS

Leveraging the Metasploit framework, configure and run the following module against the affected service:

```
auxiliary/scanner/ipmi/ipmi_dumphashes
```

SECURITY IMPACT

CVSS3.1

10.0

The ability to extract cleartext passwords presents a significant security risk, as an attacker could leverage this information to gain unauthorized remote access to sensitive services, including Secure Shell (SSH), Telnet, or web-based interfaces. Such unauthorized access could enable configurations manipulation, negatively impacting the availability and integrity of services provided by the compromised server(s).

REFERENCES

What Is IPMI And Why You Should Care

IPMI Cipher Suite Zero Authentication Bypass

Finding and Fixing Vulnerabilities in Multiple Vendor IPMI cipher zero Authentication Bypass

Frequency of occurrence: 4.1%

07 WINDOWS RCE (ETERNALBLUE)

EternalBlue is a remote code execution vulnerability in the Microsoft Server Message Block (SMBv1) protocol. It allows an attacker to send specially crafted packets to a vulnerable system, enabling unauthorized access and execution of arbitrary code with system-level privileges.

RECOMMENDATIONS

To mitigate the risk associated with the EternalBlue vulnerability, it is imperative to promptly apply the relevant security patches to all affected system(s). Additionally, a thorough review of the organization's patch management program should be conducted to identify any deficiencies that led to the unpatched status of these systems. Given the high risk and prevalence of exploitation of this vulnerability, immediate remediation efforts are crucial.

REPRODUCTION STEPS

Leveraging a tool such as Metasploit, use the smb_ms17_010 module to scan for this vulnerability.

SECURITY IMPACT

CVSS3.1

9.8

By exploiting the EternalBlue vulnerability, an attacker could gain full control over the affected system. This typically leads to additional attacks within the organization, including extraction of cleartext passwords and hashes, along with lateral movement within the network. Since exploitation of this vulnerability does not require privilege escalation on the affected system, an attacker would typically have as much access as they need on the compromised system to start enumerating the system.

REFERENCES

Security Update for Microsoft Windows SMB Server (4013389)

Frequency of occurrence: 3.8%

08 WINDOWS RCE (BLUEKEEP)

During testing, systems were identified that are vulnerable to CVE-2019-0708 (BlueKeep), which is a vulnerability that exists in Microsoft Windows systems. This vulnerability is extremely valuable to an attacker due to the availability of tools and code that could take advantage of this weakness. Successful exploitation of this vulnerability typically results in full access to the exploited system(s).

RECOMMENDATIONS

It is critical to promptly apply all relevant security updates to the affected system(s) to mitigate the BlueKeep vulnerability. Organizations should conduct a thorough review of their patch management processes to identify factors contributing to the absence of timely updates. Given the exploitability of this vulnerability and its ability to severely compromise systems, an immediate response is essential to safeguarding the organization's digital environment.

REPRODUCTION STEPS

Using a tool such as Metasploit, use the following module:

```
exploit/windows/rdp/cve_2019_0708_bluekeep_rce
```

Provide the necessary IP address information about the source and target and type "exploit" to launch the exploit. It should be noted that exploitation of this issue could potentially cause an impact on the availability of the remote system.

SECURITY IMPACT

CVSS3.1

9.8

By exploiting the BlueKeep vulnerability, an attacker could gain full control over the affected system. This typically leads to additional attacks within the organization, including extraction of cleartext passwords and hashes, along with lateral movement within the network. Since exploitation of this vulnerability does not require privilege escalation on the affected system, an attacker would typically have as much access as they need on the compromised system to start enumerating the system.

REFERENCES

Remote Desktop Services Remote Code Execution Vulnerability

Frequency of occurrence: 1.4%

09 FIREBIRD SERVERS ACCEPT DEFAULT CREDENTIALS

Default credentials are often hard-coded usernames and passwords intended for initial setup and should be changed promptly to maintain security. This issue arises when systems are deployed without reconfiguration or when default settings are overlooked during the setup process.

RECOMMENDATIONS

To mitigate this vulnerability, it is essential to utilize the GSEC tool to change the default credentials associated with Firebird servers. Additionally, implementing a policy for regular credential audits and ensuring that all default settings are modified before deployment can further enhance security. Continuously monitoring server access logs for unauthorized attempts and enabling alerts for suspicious activities will aid in detecting potential exploitations early.

REPRODUCTION STEPS

Connect to the Firebird server on port 3050 with the username 'SYSDBA' and the password 'masterkey'. On Linux, this can be achieved by using the isql-fb tool to create a database on the target:

```
# isql-fb SQL> CREATE DATABASE
'<host_ip>/3050:C:\firebird_default_creds_test.txt' user
'SYSDBA' password 'masterkey';
```

If the command completes without errors, the remote Firebird server is configured with default credentials. Make sure the database file does not already exist on the target, otherwise the following error is expected:

```
I/O error during "CreateFile (create)" operation for file "
<database_filename>"
-Error while trying to create file
-Access is denied.
```

To remove the created database, run the following command in isql-fb:

```
SQL> drop database;
```

SECURITY IMPACT

CVSS3.1

9.0

The reliance on default credentials for Firebird servers can lead to unauthorized access, allowing attackers to authenticate and conduct reconnaissance on the affected systems. They could enumerate files or alter system configurations, thereby opening pathways to further exploitation. If the attacker identifies the location of Firebird database files, they may gain the ability to read or modify sensitive database information. Furthermore, certain versions of Firebird can be manipulated to execute system commands, thereby extending an attacker's control over the remote host.

REFERENCES

Server configuration and management

Frequency of occurrence: 1.2%

10 ACTIVE DIRECTORY CERTIFICATE SERVICES PRIVILEGE ESCALATION VULNERABILITIES

The Active Directory Certificate Services (AD CS) Elevation of Privilege vulnerabilities encompass a range of security weaknesses identified within Microsoft's AD CS. These vulnerabilities are predominantly attributed to insecure default permissions assigned to specific AD CS Registry keys. Under certain conditions, an attacker may exploit these flaws to gain unauthorized elevated privileges within the Active Directory ecosystem.

RECOMMENDATIONS

To remediate the vulnerabilities associated with AD CS ESC, it is critical for organizations to promptly implement any relevant security patches and updates issued by Microsoft. Additionally, a routine review and adjustment of permissions related to AD CS Registry keys should be conducted to ensure they are correctly configured to prevent security risks. Enforcing principles of least privilege, limiting access to sensitive resources, and instituting robust monitoring for anomalous activities will further fortify defenses against potential negligence stemming from these vulnerabilities.

REPRODUCTION STEPS

Identify the target AD CS server and the specific vulnerability (e.g., ESC1 through ESC8) to exploit. From here, leverage the command line tool 'certipy' to enumerate vulnerabilities. Refer to the references section for additional walkthrough instructions.

SECURITY IMPACT

CVSS3.1

10.0

Exploitation of one or more of the identified vulnerabilities could enable an attacker to elevate privileges from lower-tier accounts to gain higher-level access within the Active Directory structure. Such access could facilitate the retrieval of sensitive, proprietary, or classified data residing within the network. Furthermore, compromised certificate services could lead to significant integrity and security breaches across the entire infrastructure, allowing threat actors to manipulate or misuse the services fundamentally.

REFERENCES

Abusing Active Directory Certificate Services

Securing AD CS: Microsoft Defender for Identity's Sensor Unveiled

ANALYSIS

Our analysis reveals that the root cause behind the most critical pentest findings continues to be configuration weaknesses and patching deficiencies. Alarmingly, the top 3 findings, **present in over half of all assessments**, can completely compromise an organization's network using readily available tools and basic techniques. These attacks often go undetected by most IT teams, highlighting serious blind spots in traditional defenses.

CONFIGURATION WEAKNESSES

Configuration weaknesses are typically due to improperly hardened services within systems deployed by administrators, and contain issues such as weak/default credentials, unnecessarily exposed services or excessive user permissions. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack will be relatively high.

PATCHING DEFICIENCIES

Patching deficiencies still prove to be a major issue for organizations and are typically due to reasons such as compatibility and, oftentimes, configuration issues within the patch management solution. Successful access may lead to confidential data and/or systems.

Attackers are actively exploiting common configuration flaws and patching gaps using publicly available tools that require a relatively low level of knowledge to execute. These weaknesses often provide a direct path to privilege escalation and unauthorized access, allowing threat actors to quickly infiltrate and move laterally across critical systems within an organization, often without detection.

> These two critical issues alone validate the need for frequent penetration testing. Relying on annual testing is no longer sufficient as threats evolve too quickly. Ongoing, automated pentesting delivers real-time visibility into security gaps, enabling organizations to detect and remediate vulnerabilities before they're exploited.

While vulnerability scanning is common practice for many organizations, these solutions fall short in demonstrating the true impact of security risks in a real-world attack scenario. For example, Tenable's Nessus scanner may flag LLMNR as merely an "**informational**" issue but fails to convey its potential for serious exploitation.

Quarterly or monthly network penetration testing using Vonahi's vPenTest goes beyond surface-level detection. Not only does it reveal the existence of vulnerabilities, but it also provides the context of how they can be chained together to deliver a full-scale compromise; giving organizations the insights they need to take meaningful action before it's too late.

vPENTEST

vPenTest is a leading automated network penetration testing platform that helps organizations proactively reduce security risks in real-time and prevent breaches—without the hassles of finding a qualified penetration tester. It delivers clear, actionable reports that explain identified vulnerabilities, their impact, and how to remediate them both technically and strategically. Plus, it strengthens compliance efforts with consistent, audit-ready results.

INDUSTRY RECOGNITION & CERTIFICATIONS

KEY FEATURES & BENEFITS

COMPREHENSIVE ASSESSMENTS MADE EASY

Schedule and run both an internal and external network penetration test, ensuring all potential entry points are thoroughly examined in your network infrastructure.

MIMICS REAL-WORLD ATTACKS

Our platform simulates real-world cyber attacks, providing you with valuable insights into your security posture and readiness against malicious actors.

TIMELY AND ACTIONABLE REPORTING

The automated testing is followed by detailed, yet easy-to-understand reports, highlighting vulnerabilities, their potential impact, and recommended actions for mitigation.

ONGOING PENETRATION TESTING

Test your network monthly without breaking the bank, ensuring that your security posture remains proactive and responsive to new threats.

EFFICIENT INCIDENT RESPONSE

By identifying vulnerabilities proactively, you are better prepared to respond to potential security incidents efficiently and effectively.

COMPLIANCE ALIGNMENT

Our solution aligns with regulatory compliance requirements, such as SOC2, PCI DSS, HIPAA, ISO 27001, as well as cyber insurance requirements for network penetration testing.

VONAHI SECURITY

TAKE YOUR SECURITY TO THE NEXT LEVEL IN 3 EASY STEPS:

01

Check Out Our Website

Visit our website and learn more about why 20K organizations love vPenTest.

▶ www.vonahi.io

02

Check Out Our G2 Reviews

See why we're the leader for penetration testing on G2 with over 180 product reviews from IT teams around the world.

▶ See G2 Product Reviews

03

Schedule a Demo

Let us show you how easy it is to use our platform to proactively identify your risks to cyberattacks in real-time

▶ Schedule a Demo

ABOUT US

Vonahi Security is a cybersecurity company that developed vPenTest, a SaaS platform that automates network penetration testing, a valuable service that mimics the way a hacker would target an organization to obtain confidential information. Through automation, our platform delivers monthly pentesting at a fraction of the cost of an outsourced consultant. We eliminate inefficiencies, increase the scope, free up budget for other cybersecurity initiatives, and ultimately make your organization more secure.

www.vonahi.io

HELLO WORLD. MEET AUTOMATED NETWORK PENTESTING.

VONAHI SECURITY

A Kaseya COMPANY

www.vonahi.io

sales@vonahi.io

@vonahisec