THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

Dat

One of the
RSM team

Attack vectors report 2024

Contents

Introduction

An effective offensive security testing strategy is of the utmost importance to all organizations in protecting sensitive data and critical systems, maintaining efficient operations and complying with evolving regulatory demands. Gaining insight into where common vulnerabilities exist is a critical element in developing a practical and sound cybersecurity stance. To that end, RSM US LLP's annual Attack Vectors Report provides a glimpse into cybersecurity strengths and weaknesses through an analysis of internal penetration tests conducted between 2021 and 2023.

Internal penetration testing involves a cybersecurity consultant (or team of consultants) posing as an attacker who gains access to an organization's internal network, either by breaching the external perimeter (such as through guessing employees' credentials) or by already having access (such as an employee, third-party contractor with malicious intent or an internal system compromise). With an initial foothold in the network, the simulated attacker searches for vulnerabilities or misconfigurations and tries to access sensitive information and systems through whatever means are available. If an organization doesn't have sufficient protections, detection and response mechanisms in place, the penetration tester may be able to compromise administrative accounts and access sensitive or confidential data. This process helps reveal what a real-world attacker may be able to achieve.

The goal of this report is to identify trends within our findings that reveal the most common issues affecting organizations' cybersecurity posture and to provide recommendations that can reduce the likelihood of business disruptions and data theft.

Key takeaways

Attackers follow the path of least resistance. This approach can result in exploiting different vulnerabilities or misconfigurations depending on the organization's size, complexity and the industry they are trying to compromise. Based on this premise, RSM tried to identify commonalities among our middle and upper market clients out of around 500 internal penetration tests conducted from 2021–23. We found that the most critical and high vulnerabilities[1] existed in the following domains:

Digital identity: One frequent vector for data breaches involves attackers exploiting previously compromised credentials. Using these stolen credentials, attackers can often remain undetected for extended periods, sometimes lasting months or even years. This approach allows them to methodically steal data and expand their access to other systems, including those with high-level privileges, without setting off many alerts or causing disruptions. Our analysis of internal penetration tests results showed that most internal network compromises by our consultants were performed by abusing some bad practices related to digital identity management and access controls. The most relevant issues are a lack of internal multifactor authentication when using privileged accounts, use of privileged user accounts for day-to-day tasks and use of weak/easy-to-guess passwords.

Configuration management: Attackers frequently exploit network vulnerabilities by capitalizing on misconfigurations that improperly extend trust to low-privileged users within an organization. A notable weakness often identified by our testers involves the capacity of authenticated internal users to request credentials, such as certificates or tokens of high-privileged users or service accounts. If not configured correctly, these oversights can enable low-privileged users to gain administrative access across the network and systems.

[1] Critical and high vulnerabilities are those which provide intruders with remote privileged user access to systems or to sensitive data

Key takeaways

Vulnerability management: While most organizations now recognize the importance of applying critical patches to their systems and have established robust patching processes, gaps remain. Our testers frequently discover that some systems miss critical patches, which could allow attackers to escalate privileges by exploiting vulnerabilities to access sensitive credentials. Notably, vulnerabilities like EternalBlue and BlueKeep on Windows systems are common targets due to their prevalence and impact. Often, the root cause of this vulnerability stems from inadequate asset management, the presence of shadow IT or suboptimal vendor management practices, leading to vendor systems that go unpatched and unmonitored for extended periods.

Architecture: The network perimeter traditionally serves as an organization's first line of defense. However, the rise of cloud technologies, SaaS and web-enabled productivity suites like Microsoft 365 and Google Workspaces has transformed and complicated this perimeter, often making it difficult for organizations to determine their exposure to the internet. Internally, the architecture becomes crucial as a final safeguard when other defenses fail. It can mitigate risks associated with misconfigurations, unpatched systems, and inadequate identity and access management. A commonly identified vulnerability by our testers in many client environments is the presence of a "flat" internal network architecture. This setup allows internal users unrestricted communication across all systems, facilitating lateral movements and potentially leading to the compromise of critical systems and data.

Notably, critical-rated vulnerabilities were identified in over a third of our internal penetration tests. While the presence of critical-rated vulnerabilities does not capture the full risk posture of the environment and does not always lead to a compromise of sensitive data, it does suggest that organizations continue to struggle to maintain consistent processes in foundational security practices. This is further emphasized by the fact that only 16.4% of these tests didn't result in at least one high or critical vulnerability.

Additional statistics include:

Tests found an average of **8.2 vulnerabilities.**

Only 1.6% of our sample yielded no vulnerabilities.

Ultimately, organizations need to take a risk-based approach to cybersecurity. This analysis provides detail and insight into the prevalence of vulnerabilities in order to establish baseline recommendations for enhancing technical security in key control areas.

Digital identity

Overview

Digital identity is a foundational component of building a robust security program. Vulnerabilities in this category indicate that current access restrictions are not sufficient, allowing users with no legitimate need for additional or escalated privileges.

Trends

Of all RSM's offensive security engagements included in our analysis, 19.5% yielded at least one digital identity vulnerability. In addition, 50.5% of that segment had at least one vulnerability deemed a high or critical risk.

19.5%

at least one digital identity vulnerability

50.5%

at least one vulnerability deemed high or critical risk

Most relevant issues

Among the most relevant vulnerabilities in this area, the ones seen most frequently include the following:

Excessive privileges

Digital identity vulnerabilities are often the result of excessive account privileges; for example, domain users having local administrator rights on their workstations or an organization having a larger number of domain administrators than is necessary to perform that level of administrative tasks. These issues result from a failure to follow the "principle of least privilege," which means that users and accounts are given only the minimum level of privileges necessary to complete their intended job or function. In this way, an organization's attack surface is reduced as much as possible since attackers need to find and compromise one of a much smaller number of privileged accounts to achieve their goal.

Default or repeated credentials across systems

In our assessments, we frequently encountered instances where default passwords were still active on third-party software or passwords were reused across multiple systems. A common example includes the reuse of built-in administrator account passwords in Windows-based environments, often justified by the ease of management. However, these practices create significant vulnerabilities. Attackers can easily compromise these passwords once they gain initial access through a server with a default password from poorly managed third-party software. Such security lapses are straightforward for attackers to exploit, potentially allowing them access to sensitive information or critical functionalities that could threaten the organization's operational integrity and reputation.

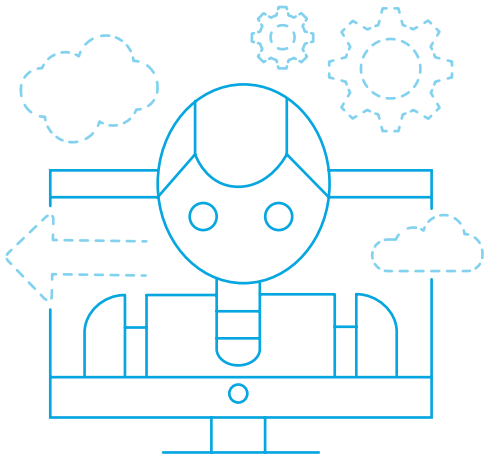
Most relevant issues (cont.)

Computers with administrative rights over other computers

Several organizations had computers with administrative rights to other computers within their environment. Computer objects, like user accounts, can be assigned permissions, including local administrator access. If a computer account with administrator privileges to other computers is compromised by an attacker, they could also gain administrative privileges over the victim computer as well—along with any sensitive data to which the victim computer has access.

Password policy

In some instances, we found organizations with weak password policies or policies not universally enforced throughout their networks. For example, a password policy that allows a smaller number of characters and does not require complexity or regular password changes can lead to users having passwords that are much easier to guess. However, even if a password policy has strong requirements, the risk is still virtually the same if insecure passwords can remain in the environment.



Recommendations

To remediate the issues described above, we recommend:

- Implementing the principle of least privilege for all users and service accounts
- Changing default passwords and utilizing password management tools, particularly for administrator accounts
- Removing computer-to-computer administrative relationships
- Enforcing a strong password policy with the following characteristics:
  - A minimum of 12 characters, or 15 for administrators
  - A mix of uppercase letters, lowercase letters, numerals and special characters
  - A time limit before passwords expire and must be changed
  - A lockout policy for repeated incorrect password attempts
- Enforcing internal multifactor authentication for privileged users
- Rotating service accounts passwords and secrets on a regular basis and using a privileged access management solution to automate this process

A strong digital identity program can also help mitigate and prevent many common access control vulnerabilities. This program should include maintaining detailed policies and procedures, performing regular access reviews and implementing mechanisms for multifactor authentication and privilege management.

Vulnerability management

Overview

To address security and operational flaws, vendors release firmware and software patches so that affected systems can be updated accordingly. When these patches are not installed, systems remain vulnerable to known security issues. Depending on how critical the issue is, even rudimentary hackers may be able to exploit the missing patch and gain full access to affected systems. Missing patches not only expose systems to increased risk of compromise, but it can also lead to compliance risks, as many regulatory and compliance frameworks require that patches be applied within a defined timeframe.

Trends

Patch management deficiencies continue to be one of the most consistent—and most exploited—issues in the past several iterations of RSM US LLP's Attack Vectors Report. This is because systems with missing patches are low-hanging fruit for attackers, making them more likely to be attacked and potentially compromised. We continue to see that critical patches have not been consistently deployed across networks, even years after patches were initially released.

Over half (51%) of the internal penetration tests included in our analysis had at least one patch management vulnerability. Just over 40% had two or more distinct vulnerabilities in this category, with some having as many as seven or eight.

The impact of missing patches can be severe when it comes to the potential for compromise. During our penetration tests, we were able to exploit missing patches as a way to:

- Gain an initial foothold into a network
- Remotely execute code on sensitive systems
- Pivot throughout the network
- Retrieve sensitive data (such as user credentials, network information and company data)
- Compromise the corporate domain
- Access environments that were intended to be segmented from the rest of the network

51%

had at least one patch management vulnerability

over 40%

had two or more distinct vulnerabilities in this category

Most relevant issues

Frequent vulnerabilities identified in this category fell into the following two groupings.

Microsoft patches

Because Microsoft Windows systems are prominent in corporate environments, missing Microsoft patches can easily become a major concern for organizations that do not have a formal patching process. When Microsoft patches are missing, an attacker may attempt to exploit vulnerabilities that have not been remediated in the version in use.

Patches that address remote code execution are of particular importance. For example, in April 2023, an elevation of privilege vulnerability was discovered in Microsoft's MSMQ service. This vulnerability allows an uncredentialed user to bypass the authentication process entirely by sending a malicious MSMQ packet to the server running the MSMQ service. Once the bypass is complete, an attacker can execute arbitrary code or commands on the remote system, typically resulting in taking control of the system and launching further attacks.

Additionally, we continue to see (and exploit) vulnerabilities—such as MS17-010 (EternalBlue), BlueKeep, and ZeroLogon—for which patches have been available for several years. In the case of MS17-010, an exploit was made public in April of 2017 and famously used in the WannaCry ransomware attack. The exploit takes advantage of a flaw in Windows' SMB that allows an attacker to remotely execute code on affected devices with NT AUTHORITY/SYSTEM privileges. Furthermore, this vulnerability can be exploited without requiring authentication or credentials, making network access the only prerequisite for exploitation.

BlueKeep (CVE-2019-0708) is related to flaws in the remote desktop protocol (RDP) service. A publicly available exploit for this vulnerability was released in September 2019. Through this exploit, an attacker can remotely execute code on affected devices with system privileges. This means the device is fully compromised without requiring user interaction or credentials. A patch for this vulnerability was released in May 2019, but our data shows that many organizations still have systems without this important patch.

Likewise, in 2020, an elevation of privilege vulnerability affecting the Netlogon Remote Protocol interface was discovered. Zerologon, as it is called, allows an uncredentialed user to bypass authentication and connect to remote systems. From there, they can execute a variety of calls, such as password changes, in order to gain control over target systems or a whole network.

Third-party patches

Missing third-party (non-Microsoft) patches is another serious deficiency in an organization's network since they can affect remote access software, IT management software, monitoring platforms and other important tools used throughout a network. In our tests, we were able to exploit missing third-party patches to gain access to sensitive systems, retrieve sensitive data or network information from those systems or make unauthorized modifications to the systems.

Identifying third-party patches as they are released by vendors may not be as straightforward as Microsoft patches, which is why many organizations struggle to maintain a consistent process for tracking and deploying them. Still, this important process should not be overlooked since attackers could exploit missing third-party patches to gain elevated privileges, trigger a denial of service vulnerability or execute arbitrary code.

Recommendations

Robust, consistent and repeatable patch management processes are a fundamental component of an effective cybersecurity strategy. Applying critical missing patches is an essential way to harden systems. Applying patches in a timely manner helps protect systems against unauthorized access, thus helping secure the data that lives in those systems and the processes that rely on those systems.

Specifically, your patch management process should include procedures for the following:

- Identifying newly released patches
- Testing patches
- Deploying patches during defined windows or based on criticality
- Rolling back patches, if necessary
- Emergency patching

Moreover, organizations should ensure patch management procedures include both Windows and third-party software. Furthermore, in cases where systems cannot be patched, organizations should look to implement compensating controls, such as segmentation, access restrictions, logging and monitoring.

Unsupported technology

Overview

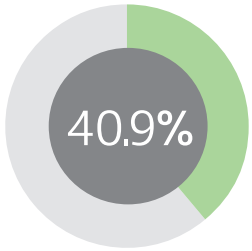
Software vendors often maintain multiple versions of their products. While releasing upgraded versions, they will continue to support previous versions of the products by providing security patches and bug fixes so that customers can continue to use them. Eventually, though, the vendor will deem many of their older products and software versions obsolete and cease providing support for them. As a result, users may continue to use those versions but will not receive patches or fixes for new vulnerabilities that may arise.

Trends

Because unsupported systems are no longer maintained by the vendor, these versions are likely to contain security vulnerabilities, with this likelihood increasing over time. New threats emerge continually, and attack techniques are constantly evolving. Unsupported systems are particularly vulnerable to these threats (like ransomware) since they can no longer receive new patches.

Moreover, unsupported technology can often be easily identified through network reconnaissance and enumeration. If an attacker identifies such systems and can determine which version is in use, they can refine their techniques to target that version and leverage any known exploits.

Of the internal penetration tests included in our analysis, 40.9% had at least one unsupported technology vulnerability. A little under one-fifth (18.1%) had two or more vulnerabilities. Windows 2000 SP4, Windows XP, Windows 7, Windows 2008 R2, and unsupported web servers such as IIS and Apache were common unsupported platforms found in our research.



of the internal penetration tests included in our analysis had at least one unsupported technology vulnerability

Most relevant issues

The most concerning issues associated with unsupported technology include:

Security flaws

The security flaws we see most often associated with unsupported technology include susceptibility to denial of service (causing the system to crash), information disclosure (leading to the discovery of useful system/user/network information), or—more critically—remote code execution (leading to a complete system takeover). Additionally, configuring unsupported technology in alignment with leading practices and industry requirements may not be possible simply because that technology may not support or accommodate that functionality.

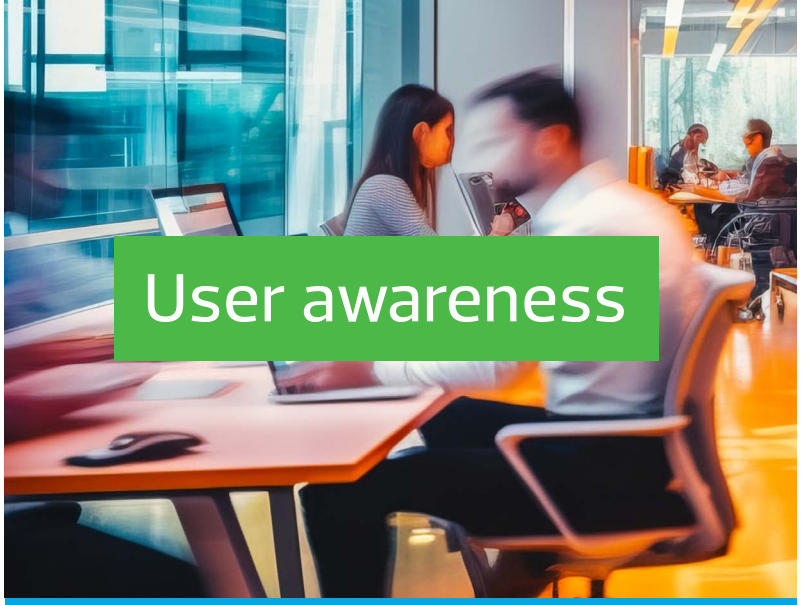
Compatibility and operational issues

Another concern with unsupported technology is that its performance may degrade over time, thus requiring more time and effort to maintain the system in alignment with business and security requirements. Furthermore, outdated technology may not be compatible with other systems in your environment, causing operational inefficiencies and making network maintenance and security more cumbersome.

Recommendations

While decommissioning or upgrading systems the moment they become unsupported is ideal, this is not feasible for many organizations, depending on the role those systems play in the environment. This is because upgrading or replacing these assets requires forethought, budget and time. Consideration should also be given to the data that the system holds and how that system supports key business processes. If the system is being replaced entirely, the new system/version needs to be tested before it is deployed.

Develop a schedule for decommissioning unsupported systems based on the risk and criticality of affected systems. Strong asset management procedures and an updated asset inventory would help organizations identify and track systems nearing the end of life. While waiting for systems to be decommissioned, organizations should implement alternative means of mitigating the risk of compromise (such as segmentation and access controls).



User awareness

Overview

Many of the vulnerabilities we regularly identify in client networks are a matter of technology weaknesses or misconfigurations. However, one of the most pervasive—and difficult to remediate—vulnerability categories is rooted in human error. This root cause, which we call "user awareness," can be just as dangerous as weaknesses in technology, and it often results from insufficient training and education of an organization's employees.

Common examples of user awareness issues include susceptibility to social engineering attacks, such as email-based phishing or voice-based vishing, and weak password selection (for example, choosing a password based on common words and patterns).

Trends

Of the internal penetration tests included in our analysis, 34.6% yielded at least one user awareness vulnerability. Out of that number, nearly a quarter of them (23.8%) had two or three vulnerabilities. In addition, 13.7% included at least one critical-rated vulnerability.

Most relevant issues

The most common issues identified in the user awareness category included three vulnerability types: weak or default passwords, the reuse of passwords between different accounts and sensitive information stored improperly.

Weak passwords

With the wealth of automated brute-forcing and password-cracking tools available, it has never been easier for a password to become compromised. Using passwords based on single words, for example, is a significant risk, as attackers can run attacks using lists of common dictionary words.

Shared passwords

In our sample set, we often found instances where the same password was shared between multiple accounts, such as two or more local administrators, or a standard user account and an administrator account. Having shared passwords is an increased risk because if an attacker manages to compromise an account with a shared password, they can now access the other account(s) as well.

Sensitive information storage

Nearly half of all tests with user awareness vulnerabilities included findings related to insecure storage of sensitive information. Often, this information—which may contain personally identifiable information, cardholder data, passwords or financial data—is stored on network shares accessible by virtually all users on a network, regardless of privilege level. Since accessing such information is typically the primary goal of an attacker, this vulnerability carries a significant risk and can lead to data theft if the attacker is able to compromise even a standard user account.

Recommendations

Our top recommendation for reducing user awareness vulnerabilities is a robust security awareness and training program. An effective security awareness program will leverage an organization's current governance model, internal tools and processes to drive employee security awareness to a more mature state. A fully optimized security awareness program should include the following:

Security awareness program ownership

Assign a qualified, dedicated resource to architect, implement, manage and provide ongoing oversight for the organization's security awareness program. Creating this role will eliminate duplication of effort, streamline workflows and lessen security costs. This will ultimately result in a holistic solution and a more robust, effective security program.

Security awareness training

Security awareness training should be included as part of the organization's onboarding process, with employee understanding reassessed at annual intervals. This training should focus on spotting and reporting sophisticated phishing attempts, data protection policies, password policies and security ethics. Employees should come away from the training with an understanding of the following:

- URL structure
- Common phishing techniques
- Company policy for reporting security incidents
- Proper storage and destruction of data
- Acceptable use policies
- Physical security, workstation, device and badge policies
- Password complexity, length and update policies

Employees should be given a quiz on the organization's security policies following the onboarding and annual training sessions to assess their level of security knowledge.

Ongoing awareness campaigns

The organization should conduct periodic awareness campaigns to refresh employees' knowledge of security policies and maintain its security posture. These campaigns can include regular newsletters, prominently displayed informational posters and security drills.

The security awareness program owner can distribute quarterly security awareness newsletters to all employees. These newsletters should provide an overview of the security policy, inform employees of any policy updates and provide relevant examples from security incidents in the news. The newsletter can also include a quiz to verify employee security awareness.

The organization should also create tailored awareness newsletters following security incidents that directly affect its assets. These will reiterate the relevant security policies and lessons learned from the incident.

Finally, the organization can also conduct phishing exercises to test employees' ability to identify phishing attacks and follow proper response procedures. These drills should be followed by a tailored awareness newsletter describing the purpose of the drill, the results and the lessons learned.

Configuration management and architecture

Overview

Network misconfigurations are among the leading root causes of vulnerabilities identified within an organization's network. Network misconfigurations are regarded as software instances or network devices which have been deployed with inappropriate or misconfigured security settings, thus increasing the risk of application or system compromise. This introduces avenues for exploration, weak encryption and cleartext passwords.

Trends

Of the internal penetration tests included in our analysis, **97.7%** yielded at least one configuration management vulnerability. Of that number, **68.4%** had five or more vulnerabilities.

Most relevant issues

The most commonly identified vulnerabilities related to network misconfigurations are excessive permissions provided to user accounts and insecure network communication protocols allowed to be used within an organization's network.

Excessive permissions

Among the most critical vulnerabilities associated with configuration management are instances when a network's user groups have excessive permissions to network resources, allowing users to read and write to domain objects. Should a malicious threat actor obtain access to a user account within such a group, they could potentially perform attacks that could grant access to domain administrator credentials or allow domain user passwords to be obtained.

With access to a domain administrator account, a threat actor could create a new user account for themselves. This would allow them consistent access to the organization's network and allow data to be removed, ransomware to be installed or further surveillance to be performed in the organization's network.

Most relevant issues, cont.

Insecure network communication protocols

In addition to excessive permissions being a critical configuration management–related vulnerability, we frequently identify that insecure network communication protocols are deployed within the organization's networks. These protocols include Internet Protocol version 6 (IPv6), Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Services (NBT-NS). Such protocols are susceptible to spoofing and poisoning attacks, often serving as the initial actions performed by a threat actor to obtain initial access to an organization's network.

Internal flat architecture

Effective architectural design is essential to mitigate risks stemming from misconfigurations, unpatched systems, and inadequate identity and access management practices. Unfortunately, a common vulnerability identified by our testers across numerous client networks is a flat network design. This design allows users comprehensive access across the network once they breach the internal perimeter, enabling them to move laterally between systems with ease. Such unrestricted access can lead to the compromise of critically sensitive systems and data.

Recommendations

As a successful remediation of network misconfigurations is often associated with disabling or altering a specific protocol, permission or feature within an organization's network, IT and cybersecurity staff should remain aware of the permissions provided to user accounts by performing regular audits and also make note of communication protocols deployed within their network. At a higher level, however, organizations are advised to follow the principle of least privilege and ensure that they use hardened minimum-security baselines that all systems within the network adhere to.

Principle of least privilege

Organizations should follow the principle of least privilege when developing user accounts or applying user permissions. This principle essentially ensures that users are only provided with the minimum degree of access necessary to perform their job duties and grants no additional access to applications or data. Applying this principle minimizes the potential damage that users could cause.

Minimum security baselines

Minimum security baselines (MSBs) are a minimum-security configuration standard to which machines should adhere and are the frontline of defense when preventing attacks. Generally, MSBs accomplish three main goals: disable unneeded features or settings, enable security features that harden the system and provide a consistent approach to system and device configuration. MSBs are often based on an authoritative body, such as NIST, CIS, SANS or a similar hardening guide. Implementing MSBs in an environment can help ensure systems are hardened and configured appropriately.

Network segmentation and microsegmentation

Network segmentation and microsegmentation are essential strategies for enhancing network security and managing risk more effectively. Segmentation involves dividing the network into distinct security zones, each corresponding to different organizational functions or data sensitivity levels, such as human resources, finance and IT departments. This configuration limits the impact of potential breaches by containing them within specific zones, thereby preventing the spread of threats across the entire network. We recommend at least dividing IT department networks from the general user population when implementing a segmentation strategy. This recommendation allows organizations to identify when a privileged user tries to connect from a non-approved network and alert on this activity.

Microsegmentation further refines this approach by implementing fine-grained traffic controls at the workload or application level within virtualized or cloud environments. It utilizes virtual firewalls and centralized policy enforcement to regulate access based on user identities, workloads and other specific attributes rather than traditional IP addresses. This method is particularly good in supporting a zero-trust security model, which assumes no implicit trust and requires verification for every access request within the network.

Segmentation and microsegmentation reduce the attack surface, simplify compliance with regulatory requirements and enhance overall security monitoring and incident management. However, these strategies require foundational IT and security practices implementation and heavy involvement from the security staff for management to ensure that security measures remain consistent and effective against evolving threats. Integration with broader security systems, such as intrusion detection and prevention, is recommended to reinforce security within segmented networks.

Insecure software development

Overview

When software is either developed or further customized by an organization in-house, there is an increased risk of the software not having adequate security measures taken into consideration. This is especially true if an organization's development team does not have a software development life cycle (SDLC) in place that adequately accounts for security threats, risks, regulatory requirements and data confidentiality, integrity and availability. As a result of applications not being developed securely, threat actors could attempt to exploit vulnerabilities within the software to compromise the data stored within.

Trends

Of the internal penetration tests in our analysis, 12.3% yielded at least one insecure software development vulnerability.

Most relevant issues

When reviewing the most significant vulnerabilities associated with software being developed insecurely, we identified two prominent issues: one wherein a threat actor can navigate file directories and another that would allow a threat actor to determine user accounts and technology associated with the application.

Directory path traversal

One of the most significant vulnerabilities associated with applications not being developed securely is the ability to traverse directory pathways. Directory traversal is an attack that takes advantage of an HTTP configuration, allowing attackers to access restricted directories and execute commands outside the web server's root directory. Most of the time, successful exploitation of this vulnerability leads to an attacker viewing other files on the server's file system that they were not intended to access, such as lists of local users and encrypted passwords. In some cases, attackers can even exploit this vulnerability to run commands on the underlying operating system.

Most relevant issues, cont.

Username and technology enumeration

User and technology enumeration is a security vulnerability within software that allows an attacker to determine whether a specific username or email address exists within a system. This vulnerability is often associated with login pages, registration forms or password reset mechanisms in web applications. This typically occurs when an application provides error messages to users or when a behavioral change occurs when a specific condition is not met (e.g., "Please provide the six-digit security code sent to your phone" after successful authentication or "Account not associated with this email address" when authentication does not occur).

Recommendations

To successfully remediate vulnerabilities associated with insecure software development, an organization's software development team may be required to make significant changes to the software they developed or actively support. This includes ensuring that the organization has a secure SDLC and that software communicates as little information to users as possible when authenticating users or providing error messages.

Secure software development life cycle

Security must be integrated into the SDLC. Incorporating security throughout the development process will identify security issues early, thus greatly easing their remediation or preventing them entirely. The earlier an issue is identified in the development process, the more cost-effective it is to fix. We recommend that the following elements be incorporated into the SDLC process to ensure that the application is built and maintained with security in mind:

- Threat modeling: Identify potential threats and risks.
- Security requirements definition: Outline security requirements that help to mitigate threats and vulnerabilities.
- Secure coding practices: Employ industry-accepted security guidelines when building the application.
- Security-focused peer reviews: Examine the code using a third party to identify security flaws.
- Code testing tools: Conduct regular testing to detect vulnerabilities.
- Final test: Test the application from a security perspective before public release and after major changes to the application.

Communicate minimal information in error messages

When applications provide verbose messages to users, it increases the likelihood that underlying technology that supports the network could be deduced or that a threat actor could determine which user accounts are present within the network. When a message is required for end users (error and validation messages, etc.), we advise that the minimum amount of information is provided in messages submitted to end users. This means not providing any error codes unless necessary, providing a generic message when an incorrect password is submitted when attempting to authenticate to a user account and otherwise ensuring that information regarding underlying technology is not provided to end users at any point.

Case study: Attack vectors used in compromise paths

The case study below narrates the compromise path we pursued during one of our internal penetration tests. This case study demonstrates how the most common attack vectors described throughout this report can be exploited to compromise an organization's network and access sensitive data. A compromise of this nature could allow an attacker to disrupt business functions and steal sensitive data.

Compromise narrative

At the start of testing, our goal was to identify viable attack vectors and high-value targets. We ran a tool that enumerated Windows operating systems to determine whether SMB signing was enabled. We found that many domain-joined SMB hosts did not require message signing. Additionally, through passive traffic analysis, we identified the organization's domain and additionally identified that LLMNR, NBT-NS, mDNS and IPv6 broadcast traffic were present within the organization's network. These forms of broadcast traffic are often sought out by threat actors, as poisoning attacks can be performed against the traffic.

By performing IPv6 poisoning, we were able to relay authentication to these SMB ports that do not require signing. It appeared that domain administrators within the network were also local administrators on many machines. As a result, capturing and relaying authentication from a domain administrator account provided us administrative access over about 70 machines.

Attack vectors exploited

- Configuration management
- Digital identity

After achieving local administrator rights, we were able to obtain stored secrets from each machine, such as the Local Security Authority and Security Account Manager files. Although we did not obtain these secrets from every machine we had administrative rights over, we did identify cleartext passwords of domain administrator accounts recoverable from memory. This effectively led to unauthenticated full domain compromise via misconfigurations and access management issues (IPv6 poisoning, SMB relay, excessive administrator access).

Attack vectors exploited

- User awareness
- Insecure software development

We confirmed the domain administrator access by obtaining an interactive shell on the domain controller. Using this access, we retrieved all the domain users' passwords and ran them through a password-cracking tool to perform a password audit. During this password audit, 66% of user passwords were cracked. While we reviewed these cracked passwords, we saw several instances of easily guessable passwords, such as variations of "password," season/year (Summer2023), local sports teams and the company name. Weak passwords indicate gaps in user awareness, as users have chosen passwords that do not align with leading practices.

Using these passwords, we accessed user systems and downloaded sensitive files that contained financial information and personally identifiable information. We also found that login forms on various applications could be manipulated to enumerate usernames. If we had not already compromised the network, we could have leveraged username enumeration and password attacks to target weak credentials. Any account compromised through these methods could have served as an alternative means of gaining a foothold in the environment.

Attack vectors exploited

- Patch management
- Unsupported technology

In the same network, we identified that 10 hosts were running unsupported operating systems (Windows 7) and were also missing the MS17-010 patch. Though we had already compromised the network, we demonstrated the ability to gain unauthorized access to these systems.

Conclusion

Even though the previous case study presents the most trivial way an internal attacker can compromise a network, it is important to note that our analysis has shown that many of the vectors in this report are present in most organizations. Other less common vectors also often emerge in addition to these vectors.

The results of our analysis indicate that organizations continue to struggle with a wide variety of security concerns. As shown in the case study, vulnerabilities relating to many root causes can be exploited by attackers. Cultivating a robust cybersecurity program, which includes strong security practices related to digital identity, configuration management, vulnerability and asset management, architecture and user awareness and training, is instrumental in reducing the impact of potential attacks, protecting your customers' data, and ensuring your business operations can continue uninterrupted. In addition, performing regular technical assessments—such as penetration testing, red teaming, vulnerability scanning, social engineering campaigns and risk assessments—helps ensure that your cybersecurity program operates as intended and that any gaps are identified and addressed.

RSM's security and privacy risk consulting practice has extensive experience with building robust cybersecurity programs that align with business goals, enterprise risk management processes and privacy requirements. The SPRC team also offers a wide catalog of penetration tests and other assessments to identify and remediate vulnerabilities.

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

RSM

+1 800 274 3978
rsmus.com

eb_0524_ 2438782_vector report 2024