Coauthored by:

TLP:WHITE

Product ID: AA22-137A

May 17, 2022

Weak Security Controls and Practices Routinely Exploited for Initial Access

SUMMARY

Cyber actors routinely exploit poor security configurations (either misconfigured or left unsecured), weak controls, and other poor cyber hygiene practices to gain initial access or as part of other tactics to compromise a victim's system. This joint Cybersecurity Advisory identifies commonly exploited controls and practices and includes best practices to mitigate the issues.

This advisory was coauthored by the cybersecurity authorities of the United States,[1],[2],[3] Canada,[4] New Zealand,[5],[6] the Netherlands,[7] and the United Kingdom.[8]

[Download the PDF version of this report (pdf, ###kb).]

Best Practices to Protect Your Systems

- Control access.
- Harden credentials.
- Establish centralized log management.
- Use antivirus solutions.
- Employ detection tools.
- Operate services exposed on internet-accessible hosts with secure configurations.
- Keep software updated.

TECHNICAL DETAILS

Malicious actors commonly use the following techniques to gain initial access to victim networks.[TA0001]

- Exploit Public-Facing Application [T1190]
- External Remote Services [T1133]
- Phishing [T1566]
- Trusted Relationship [T1199]
- Valid Accounts [T1078]

Malicious cyber actors often exploit the following common weak security controls, poor configurations, and poor security practices to employ the initial access techniques.

- **Multifactor authentication (MFA) is not enforced.** MFA, particularly for remote desktop access, can help prevent account takeovers. With Remote Desktop Protocol (RDP) as one of the most common infection vector for ransomware, MFA is a critical tool in mitigating malicious cyber activity. Do not exclude any user, particularly adminstrators, from an MFA requirement.
- **Incorrectly applied privileges or permissions and errors within access control lists.** These mistakes **can** prevent the enforcement of access control rules and could allow unauthorized users or system processes to be granted access to objects.
- **Software is not up to date.** Unpatched software may allow an attacker to exploit publicly known vulnerabilities to gain access to sensitive information, launch a denial-of-service attack, or take control of a system. This is one of the most commonly found poor security practices.
- **Use of vendor-supplied default configurations or default login usernames and passwords.** Many software and hardware products come “out of the box” with overly permissive factory-default configurations intended to make the products user-friendly and reduce the troubleshooting time for customer service. However, leaving these factory default configurations enabled after installation may provide avenues for an attacker to exploit. Network devices are also often pre-configured with default administrator usernames and passwords to simplify setup. These default credentials are not secure—they may be physically labeled on the device or even readily available on the internet. Leaving these credentials unchanged creates opportunities for malicious activity, including gaining unauthorized access to information and installing malicious software. Network defenders should also be aware that the same considerations apply for extra software options, which may come with preconfigured default settings.
- **Remote services, such as a virtual private network (VPN), lack sufficient controls to prevent unauthorized access.** During recent years, malicious threat actors have been observed targeting remote services. Network defenders can reduce the risk of remote service compromise by adding access control mechanisms, such as enforcing MFA, implementing a boundary firewall in front of a VPN, and leveraging intrusion detection system/intrusion prevention system sensors to detect anomalous network activity.
- **Strong password policies are not implemented.** Malicious cyber actors can use a myriad of methods to exploit weak, leaked, or compromised passwords and gain unauthorized access to a victim system. Malicious cyber actors have used this technique in various nefarious acts and prominently in attacks targeting RDP.
- **Cloud services are unprotected.** Misconfigured cloud services are common targets for cyber actors. Poor configurations can allow for sensitive data theft and even cryptojacking.
- **Open ports and misconfigured services are exposed to the internet.** This is one of the most common vulnerability findings. Cyber actors use scanning tools to detect open ports and often use them as an initial attack vector. Successful compromise of a service on a host could enable malicious cyber actors to gain initial access and use other tactics and procedures to compromise exposed and vulnerable entities. RDP, Server Message Block (SMB), Telnet, and NetBIOS are high-risk services.

- **Failure to detect or block phishing attempts.** Cyber actors send emails with malicious macros—primarily in Microsoft Word documents or Excel files—to infect computer systems. Initial infection can occur in a variety of ways, such as when a user opens or clicks a malicious download link, PDF, or macro-enabled Microsoft Word document included in phishing emails.
- **Poor endpoint detection and response**. Cyber actors use obfuscated malicious scripts and PowerShell attacks to bypass endpoint security controls and launch attacks on target devices. These techniques can be difficult to detect and protect against.

MITIGATIONS

Applying the following practices can help organizations strengthen their network defenses against common exploited weak security controls and practices.

Control Access

- **Adopt a zero-trust security model** that eliminates implicit trust in any one element, node, or service, and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.[9],[10] Zero-trust architecture enables granular privilege access management and can allow users to be assigned only the rights required to perform their assigned tasks.
- **Limit the ability of a local administrator account** to log in from a remote session (e.g., deny access to this computer from the network) and prevent access via an RDP session. Additionally, use dedicated administrative workstations for privileged user sessions to help limit exposure to all the threats associated with device or user compromise.
- **Control who has access to your data and services.** Give personnel access only to the data, rights, and systems they need to perform their job. This role-based access control, also known as the principle of least priviledge, should apply to both accounts and physical access. If a malicious cyber actor gains access, access control can limit the actions malicious actors can take and can reduce the impact of misconfigurations and user errors. Network defenders should also use this role-based access control to limit the access of service, machine, and functional accounts, as well as the use of management privileges, to what is necessary. Consider the following when implementing access control models:
    - **Ensure that access to data and services is specifically tailored to each user,** with each employee having their own user account.
    - **Give employees access only to the resources needed** to perform their tasks.
    - **Change default passwords** of equipment and systems upon installation or commissioning.
    - **Ensure there are processes in place for the entry, exit, and internal movement of employees.** Delete unused accounts, and immediately remove access to data and systems from accounts of exiting employees who no longer require access. Deactivate service accounts, and activate them only when maintenance is performed.[11]
- **Harden conditional access policies.** Review and optimize VPN and access control rules to manage how users connect to the network and cloud services.

- **Verify that all machines, including cloud-based virtual machine instances do not have open RDP ports.** Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.[12]

Implement Credential Hardening

- **Implement MFA.** In particular, apply MFA on all VPN connections, external-facing services, and privileged accounts. Require phishing-resistant MFA (such as security keys or PIV cards) for critical services. Where MFA is not implemented, enforce a strong password policy alongside other attribute-based information, such as device information, time of access, user history, and geolocation data. See NSA's Cybersecurity Information on Selecting Secure Multi-factor Authentication Solutions, the National Institute for Standards and Technology (NIST) Special Publication 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management, and CCCS's Information Technology Security Guidance – User Authentication Guidance for Information Technology Systems for additional steps to take to enable in-depth authentication security.
- **Change or disable vendor-supplied default usernames and passwords.** Enforce the use of strong passwords. (See guidance from NIST.)
- **Set up monitoring to detect the use of compromised credentials on your systems.** Implement controls to prevent the use of compromised or weak passwords on your network.

Establish Centralized Log Management

- **Ensure that each application and system generates sufficient log information**. Log files play a key role in detecting attacks and dealing with incidents. By implementing robust log collection and retention, organizations are able to have sufficient information to investigate incidents and detect threat actor behavior. Consider the following when implementing log collection and retention:
    - **Determine which log files are required.** These files can pertain to system logging, network logging, application logging, and cloud logging.
    - **Set up alerts where necessary.** These should include notifications of suspicious login attempts based on an analysis of log files.
    - **Ensure that your systems store log files in a usable file format,** and that the recorded timestamps are accurate and set to the correct time zone.
    - **Forward logs off local systems to a centralized repository or security information and event management (SIEM) tools.** Robustly protect SIEM tools with strong account and architectural safeguards.
    - **Make a decision regarding the retention period of log files.** If you keep log files for a long time, you can refer to them to determine facts long after incidents occur. On the other hand, log files may contain privacy-sensitive information and take up storage space. Limit access to log files and store them in a separate network segment. An incident investigation will be nearly impossible if attackers have been able to modify or delete the logfiles.[13]

Employ Antivirus Programs

- **Deploy an anti-malware solution** on workstations to prevent spyware, adware, and malware as part of the operating system security baseline.
- **Monitor antivirus scan results on a routine basis.**

Employ Detection Tools and Search for Vulnerabilities

- **Implement endpoint and detection response tools.** These tools allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.
- **Employ an intrusion detection system or intrusion prevention system** to protect network and on-premises devices from malicious activity. Use signatures to help detect malicious network activity associated with known threat activity.
- **Conduct penetration testing to identify misconfigurations.** See the Additional Resources section below for more information about CISA's free cyber hygiene services, including remote penetration testing.
- **Conduct vulnerability scanning to detect and address application vulnerabilities.**
- **Use cloud service provider tools to detect overshared cloud storage and monitor for abnormal accesses.**

Maintain Rigorous Configuration Management Programs

- **Always operate services exposed on internet-accessible hosts with secure configurations.** Never enable external access without compensating controls such as boundary firewalls and segmentation from other more secure and internal hosts like domain controllers. Continuously assess the business and mission need of internet-facing services. Follow best practices for security configurations, especially blocking macros in documents from the internet.[14]

Initiate a Software and Patch Management Program

- **Implement asset and patch management processes** to keep software up to date. Identify and mitigate unsupported, end-of-life, and unpatched software and firmware by performing vulnerability scanning and patching activities. Prioritize patching known exploited vulnerabilities.

ADDITIONAL RESOURCES

- NCSC-UK Guidance – Phishing Attacks: Defending Your Organisation
- Open Web Application Security Project (OWASP) Proactive Controls: Enforce Access Controls

REFERENCES

[1] United States Cybersecurity and Infrastructure Security Agency

[2] United States Federal Bureau of Investigation

[3] United States National Security Agency

[4] Canadian Centre for Cyber Security

[5] New Zealand National Cyber Security Centre

[6] New Zealand CERT NZ

[7] Netherlands National Cyber Security Centre

[8] United Kingdom National Cyber Security Centre

[9] White House Executive Order on Improving the Nation's Cybersecurity

[10] NCSC-NL Factsheet: Prepare for Zero Trust

[11] NCSC-NL Guide to Cyber Security Measures

[12] N-able Blog: Intrusion Detection System (IDS): Signature vs. Anomaly-Based

[13] NCSC-NL Guide to Cyber Security Measures

[14] National Institute of Standards and Technology SP 800-123 – Keeping Servers Secured

CONTACT

U.S. organizations: To report incidents and anomalous activity or to request incident response resources or technical assistance related to these threats, contact CISA at report@cisa.gov. To report computer intrusion or cybercrime activity related to information found in this advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch at 855-292-3937 or by email at CyWatch@fbi.gov. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

Canadian organizations: report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand organizations: report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

The Netherlands organizations: report incidents to cert@ncsc.nl.

United Kingdom organizations: report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

CAVEATS

The information you have accessed or received is being provided "as is" for informational purposes only. CISA, the FBI, NSA, CCCS, NCSC-NZ, CERT-NZ, NCSC-NL, and NCSC-UK do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring.

PURPOSE

This document was developed by CISA, the FBI, NSA, CCCS, NCSC-NZ, CERT-NZ, NCSC-NL, and NCSC-UK in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.