Unpatched RDP is exposed to the internet.

An unpatched endpoint using Remote Desktop Protocol (RDP) that faces the Internet is a security hole since Hackers know that RDP is a vital part of numerous business operations, making it an excellent target for accessing the endpoint and possibly the company network. Windows 7, Windows 8, Windows 10, and Windows 11 use this protocol and could be affected by an attack. The endeavor to exploit this vulnerability could crash the host or lock out an account. (*How to Mitigate the Risks of Internet-Exposed RDP*, n.d.).

If the server is successfully exploited, an aggressor could access the corporate network and potentially attack inner systems. After gaining access to the system, we can download the SAM file and decrypt it using samdump2 tools to gain access to the password and move laterally on the network. He could also get password hashes stored in the Security Account Manager (SAM) and crack them.

The administrator can use a VPN to connect to the endpoint securely. He can also use the firewall to close port 3389. A multi-factor authenticator (MFA) can be used as another layer of security.

Remediation Action:

An administrator should patch this vulnerability as soon as possible to prevent harm from a bad actor. Still, it would be wise to shut down the server or filter the port in the firewall and only allow packet traffic from known devices.

CVSS Score: 7.5 (High)

The web application is vulnerable to SQL Injection.

A vulnerable web application to SQL injection allows the hacker to pull, modify, or delete the information in the database through SQL queries, attempting to violate cybersecurity's integrity and confidentiality principles. Every operating system hosting a web application is affected by this vulnerability. Exploiting the vulnerability could crash the host or damage the data in the back-end database. (*What Is SQL Injection?*, n.d.)

If the web application is compromised, a threat actor could access the database hosted in the server filter, modify or delete sensitive information, escalate privileges, shut down the database, execute a denial of services (DoS) attack, and access other systems.

Using a Web Application Firewall (WAF) between the web server and the Internet and antivirus could mitigate this kind of attack, but it is not a long-term measure.

Remediation Action:

Using the WAF to protect the server will give the developers enough time to improve the source code and validate every input field, protecting the website from this threat. If the company cannot afford the WAF, a database backup could help if the administrator discovers the breach and the missing data, but it is not a bulletproof measure. In this case, the best thing to do is not to expose the server to the internet until the vulnerability has been mitigated.

CVSS Score: 8.8 (High)

Default password on Cisco admin portal.

When the default password is not changed, the hacker can get the device’s password by searching the browser. In this case, the Cisco admin portal allows the hacker to access the device and the company network. Any device running Internetwork Operating System (IOS) Cisco starting at 11.3 version and later is affected. Attempting to exploit the vulnerability could crash the host or lock out an account. (*(21) Trouble in Cisco Camp Highlights Scope of Default Password Problem | LinkedIn*, n.d.)

If the hacker successfully accessed the Cisco Admin Portal, a hacker could gain access to the corporate network and potentially attack inner systems, access other systems, move laterally, modify data in transit, redirect traffic, and implement a DoS attack.

Using tools such as an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) can help detect when an intruder is trying to access the device from a different network section and execute several tasks to keep hackers away.

Remediation Action:

The administrator must immediately change the default password to prevent attackers from exploiting it.

CVSS Score: 9.3 (Critical)

Apache web server vulnerable to CVE-2019-0211.

CVE-2019-0211 is an Apache web server vulnerability that allows the attacker to execute random code with the privileges of the parent process by controlling the scoreboard. Every Unix Operating System that is hosting an Apache Web Server from version 2.4.17 to 2.4.38 is affected. Attempting to exploit the vulnerability could crash the host or lock out an account. (*NVD - Cve-2019-0211*, n.d.)

If the hacker successfully accesses the Apache Web Server, he can download the files passwd and shadow and crack them with John the Reaper. He could then gain access to the corporate network and potentially attack inner systems, escalate privileges, access other systems, move laterally, use it as a botnet to launch a Denial of Service (DoS) attack, and so on.

Using tools such as an Intrusion Prevention System (IPS) can help detect anomalies in the network and execute several tasks to keep hackers away. The firewall could block some traffic to vulnerable ports from potential threat sources and prevent the execution of malware to gain access to the system.

Remediation Action:

The vulnerability should be patched as soon as possible to prevent an attacker from exploiting it. The platform should be updated to version 2.4.39, and the users who have access to this server should implement the principle of least privilege to minimize the damage of an attack.

CVSS Score: 7.8 (High)

The web server is exposing sensitive data.

A web server with a security hole that exposes sensitive data to unauthorized network users can lead to identity theft and financial fraud. Any operating system running the vulnerable web server is affected. Exploiting the vulnerability could crash the host or damage the data. (Malik, 2023)
If the server is successfully compromised, an attacker could exfiltrate sensitive information, sell it, impersonate the victims, launch social engineering attacks, escalate privileges in the system, and use it as a botnet to launch a DoS attack, identity theft, financial fraud, and move horizontally.
Using a WAF between the web server and the Internet and antivirus could mitigate this kind of attack, but it is not a long-term measure.

Remediation Action:

The developers should validate all the input fields. The data should also be encrypted while traveling through the network using HTTPS and forced to establish a connection with secure protocols; at rest, it should be encrypted with symmetric algorithms, and the key should be on a different device. In addition, access should be restricted to prevent a hacker from executing an attack or mitigate the risk.
CVSS Score: 5.3 (Medium)

The web application has broken access control.

A web application with a broken access control allows the hacker to penetrate the system by parameter tampering or force browsing, permitting the view or editing of sensitive data, elevating privileges, and possibly accessing the corporate network. Any operating system running the vulnerable web application is affected. Endeavoring to manipulate the vulnerability could crash the host, lock out an account, or damage the data in the back-end database. (*A01 Broken Access Control - OWASP Top 10:2021*, n.d.)

If the hacker successfully accessed the Web Application, He could use Burp Suite to implement a proxy and check all the request made it to the web application when the victims attempt to login the password would be seen, he could gain access to the corporate network and potentially attack inner systems, escalate privileges, acquire and crack passwords, access other systems, move laterally, exfiltrate sensitive data, and so on.

Using a WAF between the web server and the Internet and antivirus could mitigate this kind of attack, but it is not a long-term measure.

Remediation Action:

The developers should implement access control once and reuse it throughout the application. The policy should be changed to deny access by default unless it is a public resource. Alert the administrator when a login fails and follow the OAuth standard.

CVSS Score: 7.5 (High)

The Oracle WebLogic Server is vulnerable to CVE-2020-14882.

CVE-2020-14882 is a vulnerability in the Oracle WebLogic Server that allows unauthenticated users with network access via HTTP to compromise the server and potentially gain access to the corporate network. Any system running the Oracle WebLogic Server from versions 10.3.6.0.0 to 14.1.1.0.0 can be affected. Trying to manipulate the vulnerability could crash the host or lock out an account. (*CVE: Common Vulnerabilities and Exposures*, n.d.-a)

If the hacker successfully accessed the Oracle WebLogic Server, he could gain access to the corporate network and potentially attack inner systems, escalate privileges, access other systems, move laterally, exfiltrate sensitive data, and so on.

Using tools such as an Intrusion Prevention System (IPS) and Extended Detection and Response (XDR) can help detect anomalies in the network and execute several tasks to keep hackers away. The firewall could block some traffic to vulnerable ports from potential threat sources and prevent the execution of malware to gain access to the system.

Remediation Action:

The Oracle WebLogic Server can not be exposed to the Internet. Also, TCP port 7001 should be blocked or filtered to prevent harm until the server is patched.

CVSS Score: 9.8 (Critical)

Misconfigured cloud storage.

A misconfigured Cloud Storage in AWS providing more permission than the user needs increases the attack surface for the hacker, leading to unauthorized access, data breaches, and service disruptions. Any system in which a vulnerable misconfigured cloud storage is running. Exploiting the vulnerability could crash the host or lock out an account. (Ismailov, 2024)

If the hacker successfully accessed the Cloud Storage, he could gain access to the corporate network and potentially attack inner systems, escalate privileges, acquire and crack passwords, access other systems, move laterally, exfiltrate sensitive data, and so on.

Access control lists can prevent which devices access Cloud Storage and from where; encryption can prevent data exfiltration, or antivirus software can be used to avoid an attacker exploiting the vulnerability.

Remediation Action:

The administrator should audit the provisioning process and evaluate which permissions should be added to which roles to fix the misconfiguration as soon as possible and prevent an attacker from exploiting it.

CVSS Score: 7.8 (High)

Microsoft Exchange Server is vulnerable to CVE-2021-26855.

CVE-2021-26855 is a vulnerability in the Microsoft Exchange Server that allows an unauthenticated attacker to send arbitrary HTTP requests and authenticate as the Exchange Server. The vulnerability exploits the Exchange Control Panel (ECP) via Server-Side Request Forgery (SSRF), allowing the attacker to access mailboxes and read sensitive information. Microsoft Exchange Server versions 2013, 2016, and 2019 are affected operating systems. Attempting to exploit this vulnerability could crash the host or lock out an account. (*CVE: Common Vulnerabilities and Exposures*, n.d.-b)
If the hacker successfully accessed the Cloud Storage, he could gain access to the corporate network, potentially attack inner systems, and escalate privileges. After gaining access to the system, we can download the SAM file and decrypt it using samdump2 tools to access the password, access other systems, exfiltrate, modify or delete sensitive information, move laterally, etc.
Using tools such as an Intrusion Prevention System (IPS) can help detect anomalies in the network and execute several tasks to keep hackers away. The firewall could block some traffic to vulnerable ports from potential threat sources and prevent the execution of malware to gain access to the system. Also, restricting untrusted connections or setting up a VPN can mitigate the attack.

Remediation Action:

The administrator should patch the vulnerability immediately to prevent an attacker from exploiting it.

CVSS Score: 9.1 (Critical)

References

(21) Trouble in Cisco camp highlights scope of default password problem | LinkedIn. (n.d.). Retrieved March 10, 2025, from https://www.linkedin.com/pulse/trouble-cisco-camp-highlights-scope-default-password-problem/

A01 Broken Access Control—OWASP Top 10:2021. (n.d.). Retrieved March 10, 2025, from https://owasp.org/Top10/A01_2021-Broken_Access_Control/

CVE: Common Vulnerabilities and Exposures. (n.d.-a). Retrieved March 10, 2025, from https://www.cve.org/CVERecord?id=CVE-2020-14882

CVE: Common Vulnerabilities and Exposures. (n.d.-b). Retrieved March 10, 2025, from https://www.cve.org/CVERecord?id=CVE-2021-26855

How to Mitigate the Risks of Internet-Exposed RDP. (n.d.). Retrieved March 10, 2025, from https://www.coalitioninc.com/blog/undefined/blog/remote-desktop-protocol-risks

Ismailov, S. (2024, October 19). Weaknesses in AWS IAM: An In-depth Exploration. *Medium*. https://medium.com/@shukhrat.ismailov05/weaknesses-in-aws-iam-an-in-depth-exploration-8ff4fb3a8e64

Malik, O. I. (2023, August 12). *What is Sensitive Data Exposure & How to Protect Yourself from Data Exposure*. Securiti. https://securiti.ai/blog/sensitive-data-exposure/

NVD - cve-2019-0211. (n.d.). Retrieved March 10, 2025, from https://nvd.nist.gov/vuln/detail/cve-2019-0211

What is SQL Injection? Tutorial & Examples | Web Security Academy. (n.d.). Retrieved March 11, 2025, from https://portswigger.net/web-security/sql-injection