ACME Anvils

Denver, Colorado
SOC Team

Vulnerability Plan

October 31, 2023

Overview

It has been brought to the SOC Team’s attention here at ACME Anvils that we have not been identifying and addressing the vulnerabilities within the company's environment. It is our job as the SOC Team to ensure these vulnerabilities are dealt with in a timely fashion in order to improve ACME Anvils’ security posture.

Goals

1. **Risk:** Identify the possible risk of the vulnerabilities at hand.
2. **Frequency:** Determine the rate at which the risk of the vulnerability occurs.
3. **Mitigation:** Determine the amount of time it would take to mitigate the risk.

Specifications

The vulnerabilities identified within the vulnerability plan were gathered through a meticulous assessment which included network mapping, network scanning, and vulnerability scanning of ACME Anvils’ network environment.

rlogin/rsh Service Detection

Risk: Data is passed between the rlogin/rsh client and server in plaintext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. It may also allow poorly authenticated logins without passwords. Authentication bypass as a whole is possible.

Frequency: Two instances within the past fourteen days.

Mitigation: Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead. (Immediate)

VNC Server ‘password’ Password

Risk: A VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of ‘password’. An unauthenticated attacker could exploit this and take control of the system.

Frequency: The network is at constant risk as long as the VNC server is secured with the weak password

Mitigation: Secure the VNC service with a strong password. (Immediate)

SSL Version 2 & 3 Protocol Detection

Risk: SSL 2.0 and/or SSL 3.0 are affected by several cryptographic flaws and deemed to be deprecated. An attacker can exploit these flaws to launch a man-in-the-middle attack or decrypt communications between the affected service and clients.

Frequency: Three instances within the past fourteen days.

Mitigation: Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead. (Immediate)

SSL Medium Strength CIpher Suites Supported (SWEET 32)

Risk: The remote host supports the use of SSL ciphers that offer medium strength encryption.

Frequency: Three instances within the past fourteen days.

Mitigation: Reconfigure the affected application if possible to avoid use of medium strength ciphers. (Immediate)

Unix Operating System Unsupported Version Detection

Risk: According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Frequency: Six instances within the past fourteen days.

Mitigation: Upgrade to a version of the Unix operating system that is currently supported. (Immediate)

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Risk: A file read/inclusion vulnerability was found in AJP connector. An unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Frequency: Eight instances within the past fourteen days.

Mitigation: Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later. (Immediate)

Samba Badlock Vulnerability

Risk: The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Frequency: Five instances within the past fourteen days.

Mitigation: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later. (Immediate)

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Risk: The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or launch a man-in-the-middle attack.

Frequency: One instance within the past fourteen days.

Mitigation: Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated. (Immediate)

NFS Shares World Readable

Risk: The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Frequency: Three instances within the past fourteen days.

Mitigation: Place the appropriate restrictions on all NFS shares. (Immediate)

NFS Exported Share Information Disclosure

Risk: At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on the remote host.

Frequency: Six instances within the past fourteen days.

Mitigation: Configure NFS on the remote host so that only authorized hosts can mount its remote shares. (Immediate)

ISC Bind Service Downgrade / Reflected DoS

Risk: According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response. An unauthenticated, remote attacker can exploit this to degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack.

Frequency: Three instances within the past fourteen days.

Mitigation: Upgrade to the ISC BIND version referenced in the vendor advisory. (Immediate)

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL Check)

Risk: The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Frequency: One instance within the past fourteen days.

Mitigation: Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated. (Immediate)

Conclusion

ACME Anvils’ SOC Team has been notified that there has been a lack of identification and assessment on vulnerabilities found within the company’s network. Within this vulnerability plan, we prioritized the risk, frequency, and timing of mitigation of said vulnerabilities. All vulnerabilities identified and assessed during this process were gathered through network mapping, network scanning, and vulnerability scanning of the company's environment with the goals of identifying the possible risk, the rate at which they occur, and the time needed to mitigate each vulnerability.

Sources

- https://www.tenable.com/