ACME Anvils
Denver, Colorado
SOC Team

Security Roadmap

3rd November 2023

OVERVIEW

ACME Anvils currently have been applying random widgets in order to stop-gap its security issues. The SOC Team here at ACME Anvils has been tasked with describing the current security posture of the company, including exploitable vulnerabilities, in the form of a security roadmap that covers what we can fix and/or mitigate within the next 90 days, 6 months, and 12-18 months. This roadmap will help ACME Anvils reduce risk across the organization, plan our budget appropriately, and help keep its cyber insurance premiums lower due to being able to show a more mature security posture to insurance brokers.

GOALS

1. Describe ACME Anvils current security posture, including exploitable vulnerabilities.
2. Provide a roadmap of what we can fix and/or mitigate within 90 days, 6 months, or 12-18 months.
3. Provide a Security Control Tradeoff Analysis describing the cost to implement such controls and their complexity.

SPECIFICATIONS

All controls detailed within the Security Control Tradeoff Analysis are implemented from the NIST-SP800-53r3 Control Catalog in the format of the tool provided from ACME Anvils CISO, Wiley E. Coyote. All network scanning, network mapping, and vulnerability scanning have been conducted under industry standard to identify exploitable vulnerabilities within the company's network.

VULNERABILITIES

rlogin/rsh Service Detection

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.

Control: NIST-SP800-53r3 Control RA-5

Time Frame: 90 days

VNC Server ‘password’ Password

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.

Control: NIST-SP800-53r3 Control AT-2

Time Frame: 6 months

SSL Version 2 & 3 Protocol Detection

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.

Control: NIST-SP800-53r3 Control SC-13

Time Frame: 90 days

SSL Medium Strength Cipher Suites Supported (SWEET 32)

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

Control: NIST-SP800-53r3 Control SC-13

Time Frame: 90 days

Apache Tomcat AJP Connector Request Injection (Ghostcat)

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).

Control: NIST-SP800-53r3 Control CA-8

Time Frame: 90 days to 6 months

Samba Badlock Vulnerability

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.

Control: NIST-SP800-53r3 Control CA-8

Time Frame: 90 days to 6 months

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

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.

Control: NIST-SP800-53r3 Control SC-12

Time Frame: 90 days

NFS Shares World Readable

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

Control: NIST-SP800-53r3 Control RA-5

Time Frame: 90 days

NFS Exported Share Information Disclosure

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.

Control: NIST-SP800-53r3 CA-8

Time Frame: 90 days to 6 months

Unix Operating System Unsupported Version Detection

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

Control: Operating System Patch Management

Time Frame: 90 days

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

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.

Control: NIST-SP800-53r3 Control SC-12(3)

Time Frame: 90 days

ISC Bind Service Downgrade / Reflected DoS

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.

Control: NIST-SP800-53r3 Control RA-5

Time Frame: 90 days

SECURITY CONTROL ANALYSIS

Below displays a chart of the security control analysis:

Security Control Measure			Cost of Control			Quick Win?
	Resources	Initial Cost	Maintenance	Complexity	Employee Impact	
OS Patch Management	Med	Low	Med	Med	High	Yes
Literacy Training and Awareness	Med	Med	Med	Med	High	No
Penetration Testing	High	Med	Med	High	Low	No
Vulnerability Monitoring and Scanning	Low	Low	Low	Low	Med	Yes
Cryptographic Key Establishment and Management	Med	Low	Med	Med	Low	Yes
Cryptographic Key Establishment and Management | Asymmetric Keys	Med	Low	Med	Med	Low	Yes
Cryptographic Protection	Med	Low	Med	Med	Med	Yes

CONCLUSION

The SOC Team here at ACME Anvils has recently been notified that the company has been buying and applying random widgets in order to stop-gap its security issues. We have been tasked with describing the current security posture of the company, including exploitable vulnerabilities, and providing a security roadmap to assist in resolving any issues that can be fixed and/or mitigated within 90 days, 6 months, and 12-18 months. A Security Control Analysis was demonstrated to represent the cost of implementing such controls and their complexity. The roadmap provided within this report will help ACME Anvils reduce risk across the organization, plan their budget appropriately, and help keep its cyber insurance premiums lower due to being able to show a more mature security posture to insurance brokers.