NEWSFLASH

SUPPLY CHAIN ATTACK LEADS TO BACKDOOR VULNERABILITY

NANGIA & CO LLP

What is XZ Utils Backdoor Vulnerability?

The CVE-2024-3094 vulnerability, also known as the xz supply chain attack, represents a significant security issue identified within the **xz/liblzma package**, beginning from version **5.6.0**. This flaw involves the discovery of malicious code within the upstream tarballs of xz, posing a threat to the software supply chain, especially in open-source environments. Exploitation of this backdoor may potentially grant unauthorized entry and control over compromised systems.XZ Utils is a vital data compression tool widely integrated into Linux distributions. It is utilized in compressing diverse file types like release tarballs, software packages, kernel images, and initramfs images.

Background of the Vulnerability:

A Microsoft engineer involved in contributing to PostgreSQL projects encountered performance issues on a Debian system linked to SSH. These issues were characterized by heightened CPU usage during SSH logins and errors flagged by valgrind, a memory monitoring tool. Subsequent investigation uncovered that certain versions of the xz libraries contained malicious code, highlighting the significance of **CVE-2024-3094** as a critical concern for Linux security.

Who is affected?

Linux users running XZ Utils versions 5.6.0 and 5.6.1. The following distro versions are affected:

- Fedora 41 and Fedora Rawhide
- Alpine Linux
- Arch Linux (installation medium 2024.03.01, virtual machine images 20240301.218094 and 20240315.221711, and container images created between and including 2024-02-24 and 2024-03-28)
- Kali Linux (between March 26 and 29). If Kali Linux was updated before March 26, it is not affected.
- openSUSE Tumbleweed and openSUSE MicroOS (between March 7 and 28)
- Debian testing, unstable, and experimental versions (from 5.en5.1alpha-0.1 to 5.6.1-1)

It is worth noting that no versions of RHEL and Ubuntu are affected.

How to check if you are running a vulnerable version?

To determine if your system is running a vulnerable version, execute the following command in the terminal: **xz --version**. If the output indicates version 5.6.0 or 5.6.1, consider downgrading to the secure XZ Utils version 5.4.6 Stable.

What is the risk?

The illicit insertion within the xz/liblzma library has the potential to disrupt authentication processes within SSHd through systemd, opening pathways for unauthorized entry by malicious entities. The insertion essentially creates a secret backdoor/entry-point to vulnerable systems. The backdoor is implemented through a five-stage loader that uses a series of simple but clever techniques to hide itself. The backdoor may lead to:

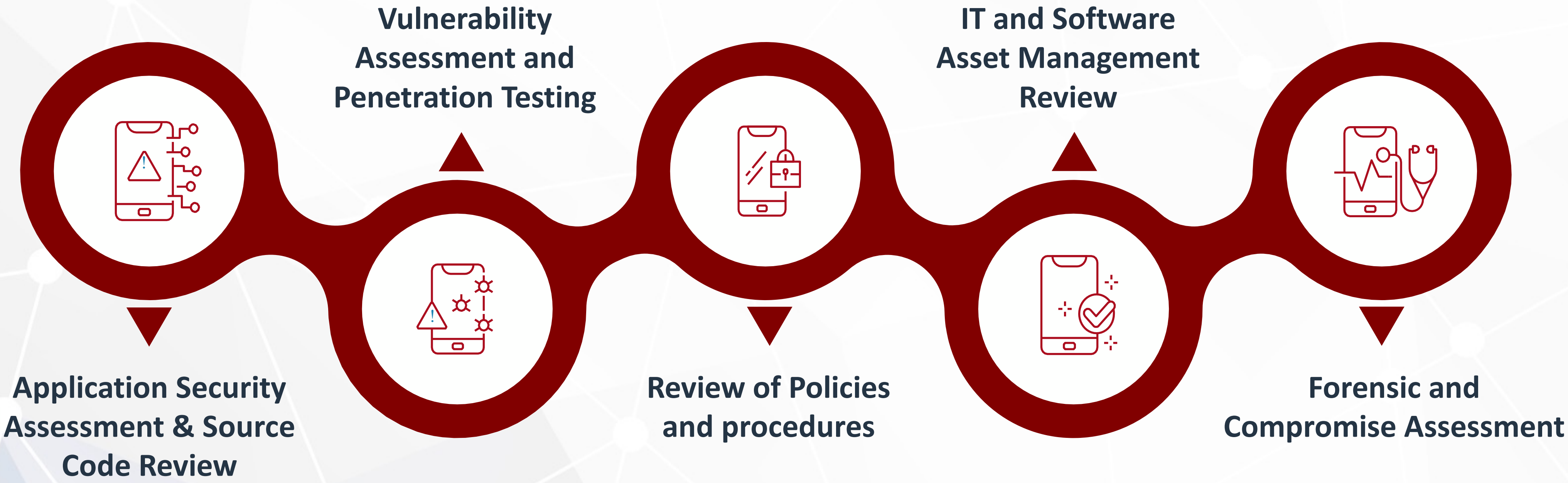
Unauthorized System Access
Denial-of-service
Data Tampering/ Exfiltration

How do you protect yourself?

Some of the steps that can be undertaken to protect your organization's infrastructure are:

1. Hardening of SSH service via measures such as strong passwords, key authentication, and monitoring for unauthorized access attempts.
2. Restrict access to public facing SSH servers entirely if possible. Else, grant access to only specific public IP addresses on need-basis.
3. Conduct regular Vulnerability Assessment and Penetration tests for all public and internal facing information systems in your organization.
4. Conduct Comprise Assessments to proactively check for any signs of compromise of your IT environment.
5. Conduct regular log monitoring to check for any unauthorized logins.
6. Additionally, check and downgrade to secure versions if running vulnerable XZ Utils versions as per the individual Operating System

How can Nangia & Co LLP help



Application Security Assessment & Source Code Review

Vulnerability Assessment and Penetration Testing

Review of Policies and procedures

IT and Software Asset Management Review

Forensic and Compromise Assessment

NOIDA

(Delhi NCR - Corporate Office) A-109, Sector - 136,
Noida - 201304, India
T: +91 120 2598000

GURUGRAM

001-005, Emaar Digital Greens Tower-A 10th Floor, Golf
Course Extension Road, Sector 61, Gurgaon-122102
T: +91 0124 430 1551

CHENNAI

Prestige Palladium Bayan,
Level 5, 129-140, Greams Road, Thousand
Lights, Chennai - 600006 T: +91 44 46549201

PUNE

3rd Floor, Park Plaza, CTS 1085,
Ganeshkhind Road, Next to Pune Central
Mall, Shivajinagar, Pune - 411005, India

DELHI

(Registered Office) B-27, Soami Nagar, New Delhi -
110017, India T: +91 120 2598000

MUMBAI

4th Floor, Iconic Tower, URMI Estate, Ganpat Rao
Kadam Marg, Lower Parel, Mumbai - 400013, India
T : +91 22 4474 3400

BENGALURU

Prestige Obelisk, Level 4, No 3 Kasturba Road,
Bengaluru - 560 001, Karnataka, India
T: +91 80 2248 4555

DEHRADUN

1st Floor, “IDA” 46 E.C. Road, Dehradun - 248001,
Uttarakhand, India T: +91 135 271 6300

www.nangia.com | query@nangia.com

The information contained in this communication is intended solely for knowledge purpose only and should not be construed as any professional advice or opinion. We expressly disclaim all liability for actions/inactions based on this communication.

Follow us at:

NANGIA & CO LLP