LAYER 9 TECHNOLOGIES

Bridging Technology and Policy

Layer 9 Technologies' analysis of the xz liblzma Vulnerability

www.layer9.tech

contact@layer9.tech

The xz liblzma Vulnerability

What Happened?

On 29 March 2024, an announcement was posted notifying the world that the Open-Source Software (OSS) package "xz-utils", which includes the *xz* data compression program and a library of software routines called "liblzma" and which is present in most Linux distributions, had been compromised. The insertion of the compromised code was done by "Jia Tan", the official maintainer of the xz-utils package. As the maintainer, the person or persons behind the "Jia Tan" identity had full access to the source code and its archives and could digitally sign installable packages such that the installed packages looked legitimate.

Some Linux distributions, commonly known as distros, make use of the "systemd" supervisory process, which uses the liblzma package, to manage *openssh*, a version of "SSH" (Secure Shell, used to remotely access and administer a system). This combination of the legitimate Linux change to openssh and the malicious compromise of xz/liblzma meant that anyone with a special backdoor key had complete, privileged access to any Linux system running that version of openssh and xz without needing login credentials.

The compromise was discovered by developer of another OSS package, Andres Freund, who noticed abnormally high CPU utilization in SSH sessions. He notified participants in an OSS security list and various Linux distro maintainers, who notified others who quickly released patches that removed the xz package with the backdoor, replacing it with an earlier version without the compromise.

Impact

This compromise would allow a remote attacker to log into any compromised Linux system as the most privileged user, granting the attack full access to the machine and any data or files residing on that machine. The attacker could replace any operating system component or, in certain circumstances, even rewrite underlying firmware to make removal

of the compromise exceedingly difficult. The compromised system could then be used by the attacker for any purpose including surveillance, participating in botnets either as a controlled node (a "zombie") or as a command-and-control node, transmitting spam, remote access of other systems, cryptomining, etc.

Am I Vulnerable?

You may be vulnerable if:

- You are running a Linux distro that uses glibc (for IFUNC)
- You have versions 5.6.0 or 5.6.1 of xz or liblzma installed (xz-utils provides the library liblzma). This will likely only be true if your Linux system is running a rolling-release distro and updating religiously.
- The combination of systemd and patched openssh is vulnerable. The backdoor payload is still being evaluated, so it is possible other configurations are also compromised.

You can check what version of xz normally comes with your distro here. Even better would be using your system package manager, which varies depending on Linux distro, to see what version is installed.

Since the compromise was only in the most bleeding edge distros and for only a short time before the package was patched, most of the Internet got very lucky.

Conclusions and Lessons

The first conclusion we can draw is that we were all extraordinarily lucky that this was caught so early. Linux is installed on a huge variety and number of critical servers, user devices, and embedded devices. A backdoor allowing access and control to all those systems would have allowed for a massive breach to public and private organizations.

Another useful takeaway is that analysis and remediation was so fast because all the source, all the package building materials, all logs, and all developer discussions were publicly available. This meant that top security researchers all over the world had access to extensive forensic information at their fingertips. While many closed-source vendors may

try to turn this exploit into a sales pitch to tout proprietary products, the reality is that OSS has many advantages beyond just cost, such as this transparency.

There is still no definitive information on the identity of the rogue maintainer "Jia Tan". We don't know their real name, who they might have been working for, or what the intended goal of the exploit was. From the long timeline in which the pieces were assembled, the familiarity with how OSS projects work, and the sophistication of the hacks, many are guessing that this is some state-run actor.

One particular area of concern is the way by which "Jia Tan" gained the trust then manipulated the original maintainer of xz-utils, who was burned out and vulnerable, to take control of the project. This should be a wake-up call to all organizations, from governments to the private sector, that while OSS may be no cost to use, it is not free as in beer; it's free like a puppy. We need to support OSS projects like xz not only with people and money, but with attention and care.

Finally, as of 3 Apr 2024, this is an active, ongoing event. The backdoor generated for SSH appears to be just one of many generated by the person(s) behind the "Jia Tan" identity. Security researchers are still going through over 700 code changes committed to OSS packages made by "Jia Tan" to see what other system services might have been targeted or what other exploits may still be out there.

Stay tuned.

Further Reading

- Official CVE
- Original email about discovery from Andres Freund
- Detailed timeline or timeline (still being updated)
- Description of backdoor components

About Layer 9 Technologies

Layer 9 Technologies, LLC is a consulting and advisory firm providing a broad range of services and expertise in Internet governance, technology policy, corporate strategy, business and operational transformations, and creation of new organizations.

With cumulatively over a century of experience in Internet technology and governance, information security, and business & program management, Layer 9 Technologies helps bridge the gap between technology and policy and brings in expertise that supports decision making and resolving policy problems.

Visit www.layer9.tech or email contact@layer9.tech for more information.