BITSIGHT

BITSIGHT SECURITY RESEARCH

# The Near Miss: Unpacking the xz library incident

Explore the critical sequence of events that almost led to a widespread cybersecurity disaster through the exploitation of the widely used xz compression library—an insightful analysis brought to you by the Bitsight TRACE security research team.

## Timeline of Events

**1. Jia Tan's Contributions**
Over three years, a developer earns trust, leading to maintainer control over the library.

**2. Patch Introduction**
A "routine" patch opens the door to exploitation.

**3. Malicious Payload Discovery**
Anomalies in performance lead to the discovery of the backdoor.

**4. Remediation**
Community and developers rally to patch and mitigate threats quickly.

## OpenSSH and Systemic Risk

**Bitsight TRACE researchers set out to answer the question:**

"How many SSH servers use OpenSSH and are running on Operating Systems that use systemd—and therefore would have eventually used the backdoored xz library in future releases?"

**38.3M**
SSH servers were identified globally in 2024.

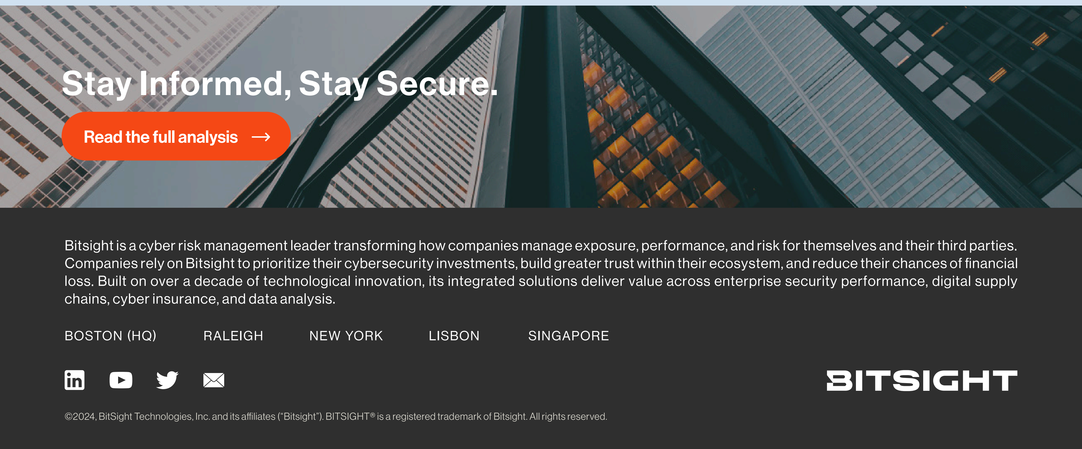
**~26M**
of identified SSH servers are running OpenSSH.

**70%**
Of SSH servers were running OpenSSH and could have been affected had the backdoor not been discovered.

**Potential widespread impact due to the ubiquity of OpenSSH in server operations.**

## "Lessons Learned"

- The importance of community vigilance.
- The need for robust maintenance protocols for open-source projects
- Rapid response capabilities to secure digital infrastructures.



## Stay Informed, Stay Secure.

Read the full analysis →

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE

BITSIGHT