PUBLICATION

Hackers Can Securely Enter Your Networks with XZ

Authors: Michael S. Klipstein
April 03, 2024

A security researcher found an intentionally placed backdoor in a software library called XZ Utils on April 2. This backdoor allows hackers to hijack secure sessions, or create their own, on devices within an organization's network. This open-sourced utility tool compresses data for easier transit and likely resides on: (1) firewalls, which act as the perimeter entrance to your network, (2) VPN concentrators, allowing you to remotely connect to your network from home or elsewhere; and (3) routers and switches, which bring the network traffic to your computer. This has the potential of being a more serious threat than the SolarWinds breach to organizations as this software is so ubiquitous. Currently, no known remediation exists and will likely require administrators to update and reconfigure software once a solution is found.

Mitigation Strategies

In response to this threat, all organizations using these access control devices should consider the following mitigation steps:

1. Identify use of XZ Utils on subcontractor and vendor devices such as firewalls, routers, switches, VPN concentrators, and management consoles for industrial control systems. Once identified consider retention of artifacts, metadata, and access logs for actions prior to any changes to the network or system.

2. Have system administrators closely monitor traffic for strange and unusual behavior such as a user attempting to access documents and files not normally accessed.

3. Update security and access policies to align with mitigations, such as permissions set for specific individuals to access sensitive data and therefore increase the difficulty for attackers.

Outside counsel can assist with reviewing your data mapping considerations, creation of security programming, disaster recovery and incident response, and further ensuring that your policies and procedures reflect the correct operating stance to protect your information and devices, as well as implementation.

For any questions about how this vulnerability might affect your business or your clients, or how you can better prepare for these types of threats, please contact Michael Klipstein Ph.D., CISM, CISSP or any member of the Baker Donelson Data Protection, Privacy, and Cybersecurity Team.