June 8, 2023

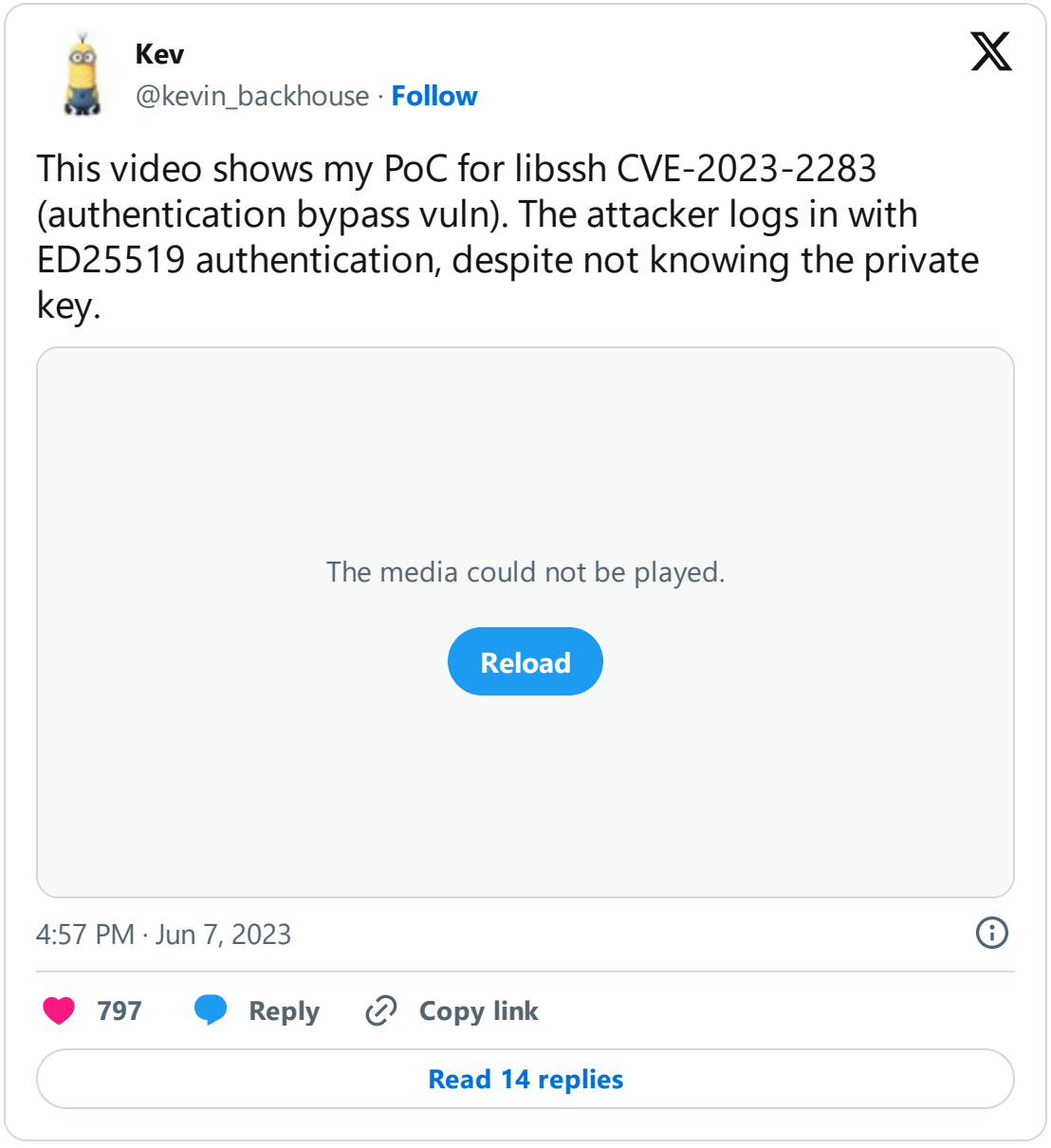
LibSSH Authentication Bypass Vulnerability (CVE-2023-2283)

What Happened?

A significant vulnerability has been identified in the libssh library, specifically within the pki_verify_data_signature function, which is used to verify connecting clients' identities. The function could allow unauthorized access under certain conditions, such as limited or insufficient memory. This issue has been identified as CVE-2023-2283. It is important to note that public proof of concept exploits have been made available, increasing the likelihood of potential attacks.

How Bad is This?

The severity of this vulnerability is considered moderate, but the public availability of exploit code significantly increases its potential impact. LibSSH is utilized by most Linux-based ssh server software, and so this impacts most major Linux distributions and likely many IoT devices as well.



Skip to content

don't need to know a password to access the system and would typically have administrator-level access. A successful exploit could lead to unauthorized access and potential misuse of sensitive data or systems.

Libssh vs OpenSSH

One important note for clarity: libssh is not the same thing as openssh.

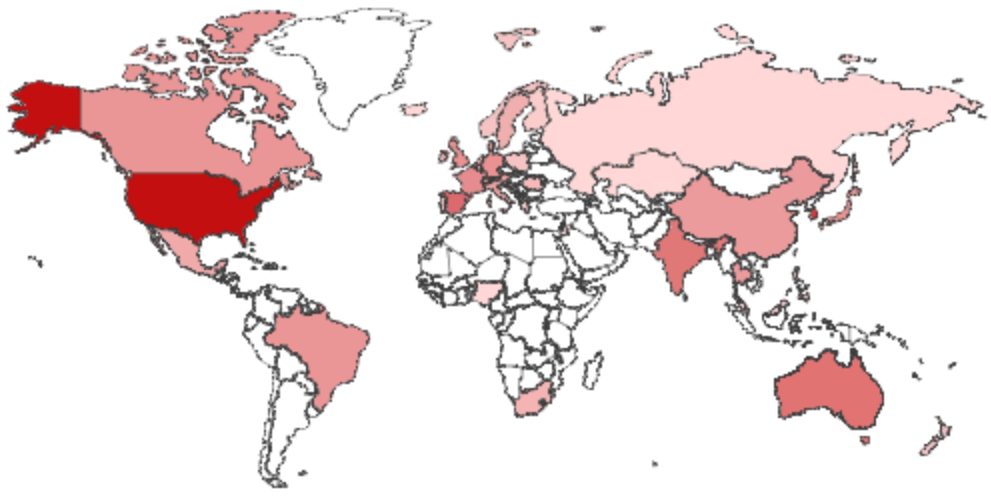
OpenSSH is a suite of secure networking utilities based on the Secure Shell (SSH) protocol, which provides secure remote login capabilities and other secure network services over an insecure network. OpenSSH is developed as part of the OpenBSD project and is included in many Unix-like operating systems. OpenSSH is widely used.

On the other hand, libssh is a multiplatform C library that implements the SSHv2 and SSHv1 protocol on client and server side. It's designed to be easy to use for developers and allows applications to provide all sorts of SSH-based functionality. libssh is not related to OpenSSH, and any vulnerabilities found in one do not necessarily apply to the other. LibSSH is less widely used.

TOTAL RESULTS

803

TOP COUNTRIES



United States	**301**
Korea, Republic of	**127**
Spain	**46**
Australia	**40**
India	**34**

Credit: Shodan.io

Per the security search engine Shodan, there are 803 exposed libssh hosts at the time of this writing; however, this number is likely much higher internally within large enterprise networks.

What Should I Do?

Skip to content

vulnerability, and it is advised that you update your libssh software to the latest version.

For Ubuntu systems, the following specific updates are available:

- Ubuntu 23.04: libssh-4 – 0.10.4-2ubuntu0.1
- Ubuntu 22.10: libssh-4 – 0.9.6-2ubuntu0.22.10.1
- Ubuntu 22.04: libssh-4 – 0.9.6-2ubuntu0.22.04.1
- Ubuntu 20.04: libssh-4 – 0.9.3-2ubuntu2.3

For other Linux distributions, please check your provider's latest security bulletins for patch availability.

How To Detect

To detect potential exploitation of this vulnerability, you may be able to monitor your system for unexpected access events, particularly any that could be related to the pki_verify_data_signature function. Further details on detection techniques and strategies may be found in the referenced articles or through your security monitoring solution's documentation.

To identify potential hosts running libssh in your network, you can use a network scanning tool like Nmap or our **Free Domain Assessment**. The following command conducts a version detection scan for SSH on all hosts within the subnet 192.168.1.0/24, and then singles out lines specifying "libssh":

```
nmap -sV -p 22 192.168.1.0/24 | grep "libssh"
```

This approach has limitations, though. It's predicated on the servers sharing a banner that explicitly names libssh. Not all servers provide such specific banners, and sometimes these banners can be misleading or incorrect. This means that despite using this command, further investigation or a manual review might still be necessary for some hosts. In case of any uncertainties, it's recommended to verify the version of libssh installed on the system.

However, our recommendation is to prioritize patching what you know you have first, then scan for anything you may not already know of.

Additional References:

- https://www.libssh.org/security/advisories/CVE-2023-2283.txt
- https://ubuntu.com/security/notices/USN-6138-1
- https://security-tracker.debian.org/tracker/CVE-2023-2283
- https://www.suse.com/security/cve/CVE-2023-2283.html

How Does Blumira Protect Against This?

Blumira's security platform includes a specific detection for SSH Connections from Public IP addresses. This detection capability is designed to identify potential scanning and attempted exploitation activities related to this vulnerability.

By continuously monitoring your network traffic, Blumira can alert your IT team to suspicious SSH connections, offering an extra layer of protection against this specific libssh vulnerability. It's another proactive measure to ensure your systems remain secure.

How Blumira Can Help

It's nearly impossible for admins to track every vulnerability, but Blumira's security experts perform threat hunting on your behalf and develop detections in real time to protect your environment.

Skip to content

Bill Reyor

More from the blog

View All Posts >

SECURITY ALERTS

6 MIN READ | JULY 1, 2024

New Unauthenticated Remote Code Execution Flaw Identified in OpenSSH Server

Read More >

SECURITY ALERTS

5 MIN READ | APRIL 12, 2024

CVE-2024-3400: Palo Alto Vulnerabilities in GlobalProtect Gateway Lead to RCE

Read More >

SECURITY ALERTS

18 MIN READ | APRIL 3, 2024

CVE-2024-3094: xz-utils (liblzma) Backdoor

Read More >

Subscribe to email updates

Stay up-to-date on what's happening at this blog and get additional content about the benefits of subscribing.

Email*

Subscribe

Products

Cloud SIEM

Endpoint Visibility

Automated Response

XDR Platform

Honeypots

Security Reports

AWS Security Monitoring

M365 Security Monitoring

Use Cases

Remote Work Security

Ransomware Prevention

SIEM For Cyber Insurance

Automated Security Operations

SOC Solutions

Microsoft Security

Industries

Healthcare

State & Local Government

Financial Services

Manufacturing

Industrial

Meet Compliance

CMMC

CJIS

SOC 2

HIPAA

NIST CSF

NIST 800-171

NIST 800-53

CIS Version 8

Cyber Insurance

FTC Safeguards

PCI DSS

Why Blumira

Pricing

Company

Integrations

Support

Careers

Resources

Blog

Free Domain Assessment

Security FAQs

Security Guides

Glossary

Webinars

Whitepapers

Videos