Zyxel security advisory for vulnerabilities of CloudCNM SecuManager

Summary

Zyxel CloudCNM SecuManager software is affected by hardcoded credentials and missing authentication vulnerabilities. We're currently working with our vendor to fix the issues and will reach out to individual customers directly to roll out the solution.

What is the vulnerability?

Multiple vulnerabilities were identified in Zyxel CloudCNM SecuManager, namely:

- Hardcoded SSH server keys
- Backdoors accounts in MySQL
- Hardcoded certificate and backdoor access in Ejabberd
- Open ZODB storage without authentication
- MyZyxel 'Cloud' Hardcoded Secret
- Hardcoded Secrets, APIs
- Predefined passwords for admin accounts
- Insecure management over the 'Cloud'
- xmppCnrSender.py log escape sequence injection
- xmppCnrSender.py no authentication and clear-text communication
- Incorrect HTTP requests cause out of range access in Zope
- XSS on the web interface
- Private SSH key
- Backdoor APIs
- Backdoor management access and RCE
- Pre-auth RCE with chrooted access

What products are vulnerable—and what should you do?

After a thorough investigation, we've confirmed that the vulnerabilities affect only CloudCNM SecuManager, a network management tool customized for specific customer demands. Other Zyxel products and services are NOT affected by the reported vulnerabilities.

CloudCNM SecuManager is co-developed with a third-party vendor. Zyxel has taken immediate action to work with the vendor to resolve the issues, making this our top priority. We'll reach out to individual customers to roll out the solution once it becomes available.

Got a question or a tipoff?

Please contact your local service rep for further information or assistance. If you've found a vulnerability, we want to work with you to fix it—contact **security@zyxel.com.tw (mailto:security@zyxel.com.tw)** and we'll get right back to you.

Source

https://pierrekim.github.io/blog/2020-03-09-zyxel-secumanager-0day-vulnerabilities.html#insecure-cloud (https://pierrekim.github.io/blog/2020-03-09-zyxel-secumanager-0day-vulnerabilities.html#insecure-cloud)

Revision history

2020-03-13: Initial release

Have a question?

We are always here to help!

Contact us **(/global/en/contact)**

Sign up for our newsletters to get the latest news!

Subscribe

Follow us on

 (https://www.facebook.com/zyxel) (https://www.linkedin.com/company/zyxel) (https://www.twitter.com/zyxel) (https://www.instagram.com/zyxelworldwide)
 (https://www.youtube.com/user/ZyXELVideo)

Support

Support Overview (https://www.zyxel.com/global/en/support)

Community

Download Library (https://www.zyxel.com/global/en/support/download)

Warranty Information (https://www.zyxel.com/global/en/support/warranty-information)

Security Advisories

Other Terms & Announcements (https://www.zyxel.com/global/en/support#announcements)

Where to Buy

Zyxel Marketplace

Locate Partners (https://www.zyxel.com/global/en/where-to-buy/locate-partner)

Distributors (https://www.zyxel.com/global/en/where-to-buy/distributors)

Newsroom (https://www.zyxel.com/global/en/newsroom)

Press Releases (https://www.zyxel.com/global/en/newsroom/press-releases)

Awards & Reviews (https://www.zyxel.com/global/en/newsroom/awards-reviews)

Newsletters

Blogs

Company

About Zyxel (https://www.zyxel.com/global/en/company/about-zyxel)

Sustainability

Success Stories (https://www.zyxel.com/global/en/success-stories)

Partner

Partner Log In

Alliance Partner