FORTINET

OUTBREAK ALERTS

Zyxel Router Command Injection Attack

Actively targeted end-of-life router in the wild

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-vulnerability-in-p660hn-t1a-dsl-cpe
CVEs: CVE-2017-18368

A command injection vulnerability (Zyxel P660HN-T1A v1) in the Remote System Log forwarder function of firmware version 3.40 (ULM.0) b3 could allow a remote unauthenticated attacker to execute some OS commands by sending a crafted HTTP request.

Background

According to the vendor advisory, a variant of Gafgyt may attempt to infect IoT devices of multiple brands, including Zyxel's P660HN-T1A router. It has been seen to leverage the outdated CVE-2017-18368 vulnerability to gain access to devices and recruit them into botnets. Zyxel provided a patch for the mentioned P660HN-T1A in 2017 how ever it continues to be on the attackers radar. The product now has reached its end-of-life.

Announced

Feb 10, 2017: FortiGuard Labs created an IPS signature to detect and block any attack attempts targeting Zyxel router vulnerability (CVE-2017-18368).

Aug 7, 2023: FortiGuard Labs continue to see attack attempts targeting the 2017 vulnerability and has blocked attack attemtps of over thousands of unique IPS devices over the last month.

Latest Developments

Aug 7, 2023: CISA added CVE-2017-18368 to its Known Exploited Catalog.

Fortinet customers remain protected by the IPS signature and recommends checking the vendor advisory to mitigate the risk completely. According to the vendor, the P660HN-T1A is a legacy product that has reached end-of-support.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery
- **Exploitation**

IPS

Detect and blocks attack attempts targeting vulnerable zyxel router (CVE-2017-18368)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 15.846	*DB 15.846*	*DB 15.846*	*DB 15.846*	*DB 15.846*

Web App Security

Detect and blocks attack attempts targeting vulnerable zyxel router (CVE-2017-18368)

FortiWeb
DB 0.00355

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiAnalyzer
DB 2.00014

Threat Hunting

FortiAnalyzer
v6.4

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response	FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training	Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

CISA Alert https://www.cisa.gov/news-events/alerts/2023/08/07/cisa-adds-one-known-exploited-vulnerability-catalog

Learn more about FortiGuard Outbreak Alerts