Zyxel Router Command Injection Attack

Actively targeted end-of-life router in the wild


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 It has been seen to leverage the outdated CVE-2017-18368 vulnerability to gain access to devices and recruit them into botnets.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 however it continues to be on the attackers radar. The product now has reached its end-of-life.

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

Latest Developments

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.

Additional Resources
- CISA Alert
- Learn more about FortiGuard Outbreak Alerts

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

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

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

FortiWeb DB 0.00355

Reconnaissance
Weaponization
Delivery
Exploitation

IPS
Web App Security
Installation

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

FortiAnalyzer DB 2.00014
FortiAnalyzer v6.4

Outbreak Detection
Threat Hunting

RESPOND
Develop containment techniques to mitigate impacts of security events:

Services that can automatically respond to this outbreak.

FortiXDR

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

Incident Response
FortiRecon: ACI
Automated Response
Assisted Response Services

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

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

NSE Training
Response Readiness

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

Security Awareness & Training
NOC/SOC Training
End-User Training

IDENTIFY
Identify processes and assets that need protection:

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

Security Rating
Know attackers next move to protect against your business branding.

FortiRecon: EASM
Attack Surface Hardening
Business Reputation