

## Zyxel Multiple Firewall Vulnerabilities

### Actively exploited and causing denial of service

<https://www.zyxel.com/global/en/support/security-advisories/zyxels-guidance-for-the-recent-attacks-on-the-zyxel-devices>  
 CVEs: CVE-2023-28771, CVE-2023-33009, CVE-2023-33010

Multiple critical vulnerabilities affecting various Zyxel devices have been seen exploited in the wild. The attackers are observed deploying Mirai like botnet inducing denial of service conditions. One of the vulnerability, CVE-2023-28771 which allows unauthenticated attackers to execute OS commands remotely has a publicly available proof of concept (PoC).

**Background** Zyxel Networks is a communications equipment company with over 100 million devices globally and serving 1 million customers according to their website. The recent discovered vulnerabilities has been seen exploited in the wild and reportedly exploited by Mirai based botnet variant to cause DDoS. As reported by FortiGuard Outbreak Alerts on December 2022, the Zyxel USG FLEX was previously targeted by the Zerobot malware due to its OS command injection vulnerability (CVE-2022-30525). According to a Shodan search there are 40,000+ Zyxel devices exposed to internet and the number of vulnerable devices could be much more as the default setting of some of the devices are not internet exposed.

**Announced** April 25, 2023: Initial release of advisory from vendor on CVE-2023-28771, CVE-2023-33009, CVE-2023-33010 <https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls>

May 31, 2023: CISA added CVE-2023-28771 to its Known Exploited Vulnerability catalog (KEV).

June 5, 2023: CISA added CVE-2023-33009 and CVE-2023-33010 to its Known Exploited Vulnerability catalog (KEV).

**Latest Developments** June 5, 2023: Mirai based botnet remain active, lately affecting multiple IoT devices. Go to Additional resources to review the Outbreaks and vulnerabilities related/affected by Mirai based Botnet.

June 5, 2023: FortiGuard added Threat Signal on Zyxel Multiple Firewall Vulnerabilities <https://www.fortiguard.com/threat-signal-report/5179/>

July 19, 2023: FortiGuard Labs released a detailed analysis blog article on DDoS botnets targeting Zyxel Vulnerability. <https://www.fortinet.com/blog/threat-research/ddos-botnets-target-zyxel-vulnerability-cve-2023-28771>

FortiGuard Labs has released an IPS signature to detect any attack attempts to exploit CVE-2023-28771 and further investigating protections for CVE-2023-33009 and CVE-2023-33010. Antivirus signatures to detect and block known malware related to exploitation of vulnerable Zyxel devices.

It is strongly recommended to update ATP, USG Flex, VPN, and ZyWALL/USG firewalls to prevent exploitation of recent vulnerabilities as per vendor advisory to fully mitigate the risk and look for DoS "Denial of Service" like symptoms that could arise if compromised. <https://www.zyxel.com/global/en/support/security-advisories/zyxels-guidance-for-the-recent-attacks-on-the-zyxel-devices>

## PROTECT

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

### Reconnaissance

#### Lure

Detects attack attempts related to Zyxel Multiple Firewall Vulnerabilities and prevents lateral movement on the network segment



FortiDeceptor  
v3.3+

#### Decoy VM

Detects attack attempts related to Zyxel Multiple Firewall Vulnerabilities and prevents lateral movement on the network segment



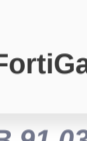
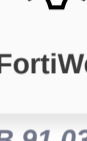
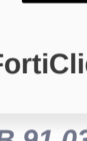
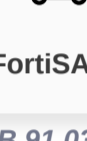
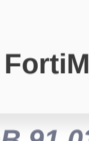
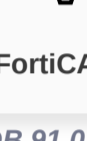
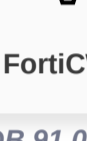


FortiDeceptor  
v3.3+

### Weaponization

### Delivery




#### AV

Detects and blocks Marai based botnet related to Zyxel vulnerabilities

 FortiGate DB 91.03837	 FortiWeb DB 91.03837	 FortiClient DB 91.03837	 FortiSASE DB 91.03837	 FortiMail DB 91.03837	 FortiCASB DB 91.03837	 FortiCWP DB 91.03837
 FortiADC DB 91.03837	 FortiProxy DB 91.03837					

#### AV (Pre-filter)

Detects and blocks Marai based botnet related to Zyxel vulnerabilities

 FortiEDR DB 91.03837	 FortiSandbox DB 91.03837	 FortiNDR DB 91.03837
--	--	--

### Exploitation

#### IPS

Detects and blocks OS Command Injection vulnerability (CVE-2023-28771)

 FortiGate DB 23.571	 FortiSASE DB 23.571	 FortiNDR DB 23.571	 FortiADC DB 23.571	 FortiProxy DB 23.571
---	---	--	--	--

### Installation




#### C2

#### Action


## DETECT

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

#### IOC



 FortiAnalyzer	 FortiSIEM	 FortiSOCaaS
--	--	--

#### Outbreak Detection



FortiAnalyzer  
DB 2.00008

#### Threat Hunting

 FortiAnalyzer v6.4+	 FortiSIEM v6.4+
---	---

#### Content Update




FortiSIEM  
DB 316

## RESPOND

Develop containment techniques to mitigate impacts of security events:

#### Automated Response



Services that can automatically respond to this outbreak.



FortiXDR

#### Assisted Response Services

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

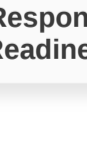
 Incident Response	 FortiRecon: ACI
--	--

## RECOVER

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

#### InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.



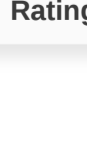
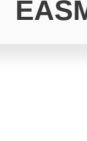
Response Readiness

## IDENTIFY

Identify processes and assets that need protection:

#### Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

 Security Rating	 FortiRecon: EASM
--	---

## Additional Resources

- Bleeping Computer** <https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-zyxel-firewall-flaw-in-ongoing-attacks/>
- SecurityWeek** <https://www.securityweek.com/zyxel-urges-customers-to-patch-firewalls-against-exploited-vulnerabilities/>
- Outbreak- Zerobot Attack** <https://www.fortiguard.com/outbreak-alert/zerobot-attack>
- Outbreak- Router Malware Attack** <https://www.fortiguard.com/outbreak-alert/router-malware-attack>
- CISA KEV Catalog** <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Shodan Search** <https://www.shodan.io/search?query=title%3A%22USG+FLEX%22%2C%22ATP100%22%2C%22ATP200%22%2C%22ATP500%22%2C%22ATP700%22%2C%22ZYWALL+USG%22>

Learn more about [FortiGuard Outbreak Alerts](#)