

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Zyxel Firewall Flaw Exploited to Unleash Helldown Ransomware Havoc

Date of Publication

December 4, 2024

Admiralty Code

A1

TA Number

TA2024449

Summary




First Seen: November 2024

Affected Products: Zyxel, USG FLEX, USG FLEX 50(W), USG20(W)-VPN series firmware

Malware: Helldown ransomware

Impact: Zyxel firewalls have been found to contain a critical vulnerability actively exploited in ongoing cyberattacks. Tracked as CVE-2024-11667, this flaw is a directory traversal vulnerability located in the web management interface of the Zyxel ZLD firewall firmware. Exploiting this vulnerability, attackers gain unauthorized access to system files and use the flaw as an entry point to deploy the dangerous Helldown ransomware, causing significant damage to targeted systems.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-11667	Zyxel Multiple Firewalls Path Traversal Vulnerability	Zyxel, USG FLEX, USG FLEX 50(W), USG20(W)-VPN series firmware			

Vulnerability Details

#1

Zyxel has released a critical security advisory addressing a severe vulnerability in its firewall products, identified as CVE-2024-11667. This vulnerability, located in the web management interface of the Zyxel ZLD firewall firmware, is a directory traversal flaw that allows attackers to gain unauthorized access to system files. Exploitation of this flaw has been linked to the deployment of [Helldown ransomware](#), resulting in widespread disruptions for affected organizations.

#2

By crafting malicious URLs, attackers can exploit the vulnerability to download or upload files, steal credentials, and establish unauthorized backdoor VPN connections. Once they infiltrate the system, attackers frequently create illicit user accounts, ensuring persistent access and enabling lateral movement within the network.

#3

The impact of these attacks has been far-reaching. The attackers' ultimate aim is often to demand ransom payments in exchange for file decryption, leaving businesses grappling with both financial and reputational damage. This highlights the critical importance of timely patching to safeguard systems against such sophisticated threats.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-11667	Zyxel ATP series Version 5.00 - 5.38, Zyxel USG FLEX series Version 5.00 - 5.38, Zyxel USG FLEX 50W Version 5.10 - 5.38, Zyxel USG20W-VPN Version 5.10 - 5.38	cpe:2.3:o:zyxel:atp_firmware:*.:*:*:*:*:* cpe:2.3:o:zyxel:usg_flex_firmware:*.:*:*:*:*:* cpe:2.3:o:zyxel:usg_flex_50w_firmware:*.:*:*:*:*:* cpe:2.3:o:zyxel:usg20-vpn_firmware:*.:*:*:*:*:*	CWE-22

Recommendations



Update: Users are strongly urged to update to ZLD 5.39 or later to address CVE-2024-11667 and benefit from enhanced security features. This update not only patches the critical directory traversal vulnerability but also strengthens overall system defenses against potential threats.



Remove Unauthorized Accounts: Immediately identify and remove any suspicious or unauthorized user accounts, such as "SUPPORT87" or "SUPPOR817," from all affected systems. Terminate all active sessions associated with suspicious accounts or originating from untrusted IP addresses to prevent further exploitation.



Restrict Access: It's crucial to review and tighten security policies to prevent unauthorized access. Remove any rules that allow unrestricted access and ensure that policies are configured to restrict WAN, LAN, and SSL VPN traffic based on the principle of least privilege.



Log Monitoring: Continuously monitor and analyze logs for any signs of suspicious activity or unauthorized access attempts. This proactive approach enables quick identification of potential threats and helps in taking immediate action to mitigate risks.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0003</u> Persistence	<u>TA0010</u> Exfiltration	<u>TA0040</u> Impact
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1486</u> Data Encrypted for Impact	<u>T1136</u> Create Account

Patch Details

Update to the latest firmware version, ZLD 5.39 or later. This update addresses the vulnerability CVE-2024-11667 helping to protect your system from potential exploitation.

Link: <https://www.zyxel.com/us/en-us/support/download>

References

<https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-protecting-against-recent-firewall-threats-11-27-2024>

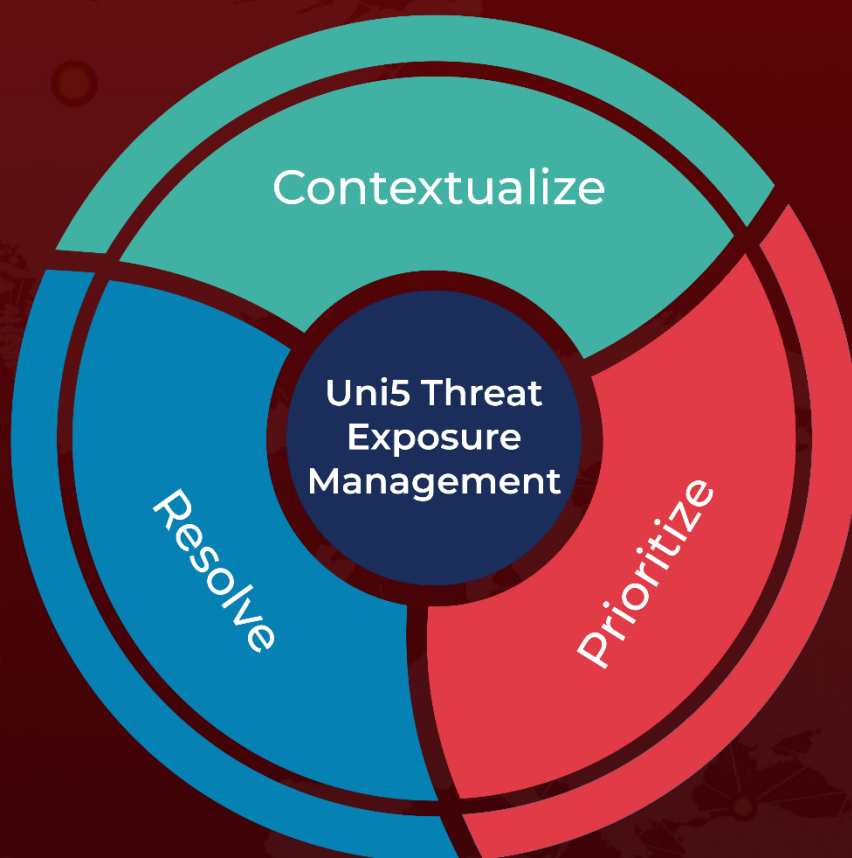
<https://cyble.com/blog/german-cert-warns-zyxel-firewalls-exploited/>

<https://hivepro.com/threat-advisory/new-helldown-ransomware-a-growing-threat-across-cross-platform-systems/>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

December 4, 2024 • 5:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com