Forensic Report

Executive summary

Zyxel Networks is aware of a recently identified issue affecting a limited number of ZLD-based firewall devices. Our investigation has identified the root cause, and Zyxel has already prepared a recovery solution to help affected customers restore their devices safely.

There is **no evidence that the latest ZLD5.42 firmware introduced this issue**. Instead, our investigation indicates that the malicious code was implanted on affected devices **before they were upgraded to the latest firmware**.

The situation is well understood, and Zyxel has prepared both a software fix and detailed recovery procedures.

What happened?

Our investigation found that attackers had **previously** gained unauthorized access to affected devices running older firmware versions that contained known security vulnerabilities. After obtaining access, the attackers implanted several malicious files into the system. These files were designed to abuse an existing system mechanism to execute the malicious program during the attack campaign.

Once running, the malicious program disguised itself as legitimate system processes and modified internal network traffic handling. As a result, some LAN users could experience symptoms such as:

- Unable to access the device's web management interface (GUI)
- HTTP/HTTPS connections from the LAN being redirected incorrectly
- Internet connectivity issues for internal users

Our investigation has identified the malicious components involved, and their behavior is fully understood - see below full forensic findings report.

Forensic findings

Indication of compromise

The following unauthorized files were found on the affected system:

```
/etc/zyxel/ftp/.dha/.dha_gecon
/etc/zyxel/ftp/.dha/.dha_gecov
/etc/zyxel/ftp/.dha/app_patr
/etc/zyxel/ftp/.dha/dha_disable_ports
/etc/zyxel/ftp/.dha/dha_geoip
```

Confirmed attack flow

The attack sequence has been confirmed as follows:

1. During normal operation, **ZLDconfig** executes the existing system script `/etc/zyxel/ftp/.dha/dha_disable_ports` as part of its execution flow.
2. The attacker abused this existing execution mechanism by replacing the legitimate `dha_disable_ports` script with a malicious version.
3. The malicious `dha_disable_ports` script subsequently launches `dha_geoip`, which in turn executes `app_patr`.
4. `app_patr` is the primary malware component responsible for the malicious activities.

Malware behavior

After execution, `app_patr` disguises itself as a legitimate system process by randomly adopting the name of an existing ZLD daemon, such as:

- `/usr/sbin/zylogd`
- `/usr/sbin/zwd`
- `/usr/sbin/uamd`
- Other legitimate ZLD daemon processes

This process masquerading is intended to evade detection by blending in with normal system processes.

Network manipulation

The malware modifies the **iptables NAT table** by creating redirection rules for traffic that meets all of the following conditions:

- **Source IP** belongs to one of the following private address ranges:
  - `10.0.0.0/8`
  - `172.16.0.0/12`
  - `192.168.0.0/16`
- **Destination port** is one of the following:
  - HTTP (TCP/80)
  - HTTPS (TCP/443)
  - Device GUI service port

Matching traffic is redirected to the local TCP port **58616**.

Impact

As a result of these malicious NAT redirection rules, HTTP, HTTPS, and device GUI connections originating from the LAN are intercepted and redirected to a listener controlled by the malware.

This causes users attempting to access the device's web management interface to experience abnormal GUI behavior or complete loss of access.

Why can this still happen on devices already running the latest firmware?

Some customers have reported that their devices were already upgraded to the latest firmware (for example, ZLD 5.42 Patch 1) before the incident was observed.

Our investigation confirms that **the latest firmware is not the source of the problem**.

The malicious code was installed **before** the device was upgraded, while it was still running an older firmware version that contained vulnerabilities which have since been fixed. Refer to **Appendix** to understand list of vulnerabilities discovered in older firmware versions and in which firmware version the vulnerability was patched.

Upgrading the firmware successfully removes the software vulnerabilities that allowed the initial compromise, but it does **not automatically remove malicious files that had already been implanted** on the system.

In other words:

- The **vulnerability has already been fixed** by the latest firmware.
- The **remaining issue is the malicious files left behind from the earlier compromise**, which require a separate cleanup process.

Recovery solution

To help customers recover affected devices, Zyxel is releasing an urgent hotfix that removes all malicious files and processes identified during this attack campaign.

In addition, Zyxel CSO will publish an official recovery procedure that includes:

- Backing up the device configuration
- Installing the recovery hotfix (DF), which removes the identified malicious components automatically
- Restoring the device configuration
- Change admin password & binding 2FA against admin accounts
- Configuring inbound ACL based on **Principle of Least Privilege (PoLP),** to restrict administrative access to the device from the Internet

Customers should follow the official recovery procedure to ensure the device is fully restored to a trusted state.

Urgent hotfix (DF) - purpose and function

The purpose of **ZLD5.42 ITS26-WK28** is to **automatically remove indicators of compromise (IOCs) and malicious files associated with the recent attack campaign** from affected devices.

Unlike the traditional recovery process—which requires physical access to the device, console access, and a factory reset to remove malicious artifacts—this hotfix can be installed remotely through the Web Configurator or uploaded locally

via the device management interface. This enables customers to remediate affected devices without dispatching personnel on-site, significantly reducing recovery time and operational costs.

What the hotfix does

During the first boot after the hotfix is installed, **ZLD5.42 ITS26-WK28** automatically searches for and removes the malicious files identified as part of this incident, including:

```
/db/etc/zyxel/ftp/.dha/.dha_gecon
/db/etc/zyxel/ftp/.dha/.dha_gecov
/db/etc/zyxel/ftp/.dha/app_patr
/db/etc/zyxel/ftp/.dha/dha_disable_ports
/db/etc/zyxel/ftp/.dha/dha_geoip

/db2/etc/zyxel/ftp/.dha/.dha_gecon
/db2/etc/zyxel/ftp/.dha/.dha_gecov
/db2/etc/zyxel/ftp/.dha/app_patr
/db2/etc/zyxel/ftp/.dha/dha_disable_ports
/db2/etc/zyxel/ftp/.dha/dha_geoip
```

These files have been confirmed as indicators of compromise (IOCs) directly associated with the malicious campaign.

Security baseline

In addition to removing the malicious artifacts, **ZLD5.42 ITS26-WK28** is built on the latest ZLD software baseline and incorporates all previously released security fixes. As a result, it includes remediation for all currently known vulnerabilities addressed in the latest ZLD release.

Current status

Our investigation has identified the attack mechanism, the malicious components involved, and the recovery process.

Zyxel is actively supporting customers worldwide by providing:

- An emergency hotfix (DF) to remove the malicious components
- Official recovery procedures

- Technical assistance as needed
- Ongoing monitoring

We recommend that customers follow the official guidance as soon as it becomes available to ensure their devices are fully cleaned and protected.

Appendix

List of high/critical vulnerabilities discovered in older firmware versions, and in which firmware the vulnerability was fixed.

CVE-2023-28771 (CVSS: 9.8 – Critical)

- Does **not** require administrator credentials.
- An attacker could obtain **root privileges** on the device.
- **Fixed in:** V5.36P0

CVE-2023-27991 (CVSS: 8.8 – High)

- Requires valid **limited-admin** account credentials.
- An authenticated attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.36P0

CVE-2023-28767 (CVSS: 8.8 – High)

- Does **not** require administrator credentials.
- An attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.37P0

CVE-2023-33011 (CVSS: 8.8 – High)

- Does **not** require administrator credentials.
- An attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.

- **Fixed in:** V5.37P0

CVE-2023-33012 (CVSS: 8.8 – High)

- Does **not** require administrator credentials.
- An attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.37P0

CVE-2023-34139 (CVSS: 8.8 – High)

- Does **not** require administrator credentials. The **Free Time WiFi Hotspot** feature must be enabled.
- An attacker could obtain **root privileges** on the device.
- **Fixed in:** V5.37P0

CVE-2023-6398 (CVSS: 7.2 – High)

- Requires valid **administrator** credentials.
- An authenticated attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.37P2

CVE-2023-6764 (CVSS: 8.1 – High)

- Does **not** require administrator credentials.
- An attacker could obtain **root privileges** on the device.
- **Fixed in:** V5.37P2

CVE-2024-42057 (CVSS: 8.1 – High)

- Requires valid **administrator** credentials.
- An authenticated attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.39P0

CVE-2024-42059 (CVSS: 7.2 – High)

- Requires valid **administrator** credentials.
- An authenticated attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.39P0

CVE-2024-42060 (CVSS: 7.2 – High)

- Requires valid **administrator** credentials.
- An authenticated attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.39P0

CVE-2024-7203 (CVSS: 7.2 – High)

- Requires valid **administrator** credentials.
- An authenticated attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.39P0

CVE-2025-8078 (CVSS: 7.2 – High)

- Requires valid **administrator** credentials.
- An authenticated attacker could obtain **root privileges** on the device.
- **Fixed in:** V5.41P0

CVE-2025-9133 (CVSS: 8.1 – High)

- Requires valid **administrator** credentials.
- The vulnerability could be exploited even when **2FA is enabled**, without completing two-factor authentication.
- An authenticated attacker could execute arbitrary system commands (e.g., `reboot`) and retrieve the device configuration.
- **Fixed in:** V5.41P0

CVE-2025-11730 (CVSS: 7.2 – High)

- Requires valid **administrator** credentials.
- An authenticated attacker could obtain **root privileges** on the device.
- **Fixed in:** V5.42P0