National Cyber Security Centre

2305260108-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical vulnerabilities in Zyxel firewalls - (CVSS 9.8)

Friday 26th May, 2023

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Zyxel has released a number of security advisories in relation to critical OS command injection and multiple buffer overflow vulnerabilities in a number of their firewall series.

The first advisory provides information and recommendations on the OS command injection vulnerability tracked as CVE-2023-28771. Exploitation of this vulnerability could allow an unauthenticated attacker to execute OS commands remotely by sending specially crafted packets to an affected device.

The second advisory provides information and recommendations on two buffer overflow vulnerabilities tracked as CVE-2023-33009 and CVE-2023-33010. An attacker could exploit these vulnerabilities to cause Denial-of-Service (DoS) conditions and remote code execution on an affected device.

Products Affected

CVE-2023-28771, CVE-2023-33009 and CVE-2023-33010 affect the following Zyxel product series:

- **ATP**
  - Versions: ZLD V4.32 to V5.36 Patch 1
- **USG FLEX**
  - Versions: ZLD V4.50 to V5.36 Patch 1
- **VPN**
  - Versions: ZLD V4.30 to V5.36 Patch 1
- **ZyWALL/USG**
  - Versions: ZLD V4.25 to V4.73 Patch 1

CVE-2023-33009 and CVE-2023-33010 affect the following Zyxel product series:

- **USG FLEX50(W) / USG20(W)-VPN**
  - Versions: ZLD V4.25 to V5.36 Patch 1

Impact

Exploitation of CVE-2023-28771 could allow an unauthenticated attacker to execute OS commands remotely by specially sending crafted packets to an affected device.

Exploitation of CVE-2023-33009/CVE-2023-33010 could allow an unauthenticated attacker to cause Denial-of-Service (DoS) conditions and achieve remote code execution on an affected device.

To date, the NCSC is aware of these vulnerabilities being exploited in the wild.

Recommendations

The NCSC recommends that affected organisations review the issued security advisories below from Zyxel and update to the latest relevant patch as soon as possible.

Further information and additional steps available to organisations can be found in Zyxel's advisories here:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-remote-command-injection-vulnerability-of-firewalls
- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie