Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Gafgyt Botnet Exploiting Five Years Old Critical Vulnerability in Zyxel Routers

Date of Publication	Admiralty Code	TA Number
August 11, 2023	A1	TA2023330

Summary

First Seen: August 7, 2023
Malware: Gafgyt botnet (aka Bashlite, Lizkebab, PinkSlip, Qbot, Torlus, and LizardStresser)
Impact: A critical vulnerability (CVE-2017-18368) in the Zyxel P660HN-T1A router allows the Gafgyt botnet to execute unauthorized commands, potentially leading to complete takeover of affected devices. This exploitation enables the botnet to launch attacks, compromise network stability, and potentially compromise sensitive data.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-18368	Zyxel P660HN-T1A Routers Command Injection Vulnerability	Zyxel P660HN-T1A Routers	✗	✓	✓

Vulnerability Details

#1 The CVE-2017-18368 vulnerability is a critical severity vulnerability that allows an attacker to execute arbitrary commands on a Zyxel P660HN-T1A router. This vulnerability was patched by Zyxel in 2017, but there are still many devices that are running the vulnerable firmware.

#2 The Gafgyt botnet is actively exploiting this vulnerability to infect Zyxel P660HN-T1A routers. Once a router is infected, it can be used to launch denial-of-service attacks, steal data, or spread other malware.

#3 Despite Zyxel's previous alerts urging users to upgrade their firmware, the attacks have persisted, with an average of 7,100 daily attacks reported by Fortinet since July 2023. The malware attempts to exploit the vulnerability to gain control over the router and recruit it into a botnet for attacking gaming servers.

#4

Zyxel has updated its security advisory to clarify that devices running the latest firmware version (3.40(BYF.11)) are immune to the attacks. However, since the P660HN-T1A router has reached its end-of-life and is no longer supported, Zyxel recommends users to replace it with a newer model for better protection. Signs of a compromised router include unstable connectivity, unexpected reboots, unusual network traffic, and configuration changes.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2017-18368	Zyxel P660HN-T1A v1	cpe:2.3:o:billion:5200wt_firmware:7.3.8.0:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply Patch: Install the security patch provided by Zyxel to address the CVE-2017-18368 vulnerability. This patch closes the security gap that allows attackers to exploit the unauthenticated command injection vulnerability.

Disable Remote Log Forwarding: Turn off the Remote System Log forwarding function on the Zyxel P660HN-T1A router. By disabling this feature, you remove the potential avenue that the malware exploits for unauthorized access.

Isolate Legacy Devices: As the P660HN-T1A router has reached end-of-life and is no longer supported, consider isolating or decommissioning these devices. Transition to newer-generation products with active security support to minimize exposure to vulnerabilities like CVE-2017-18368.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0042** Resource Development	**TA0002** Execution	**TA0005** Defense Evasion
T1584.005 Botnet	**T1584** Compromise Infrastructure	**T1059** Command and Scripting Interpreter	**T1202** Indirect Command Execution
T1190 Exploit Public-Facing Application	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	21ecc53c3fe5336dd717b50fa70e281c5612b0c770f68d9f38c93e13e8357e21, 08d221d2d98a81d85e8bf0e8f3c8c4ddb35cc32c268a2cfe2cb2837e7f8fc731, e1cb8cf85745f7a771b33eab060e04556b1b33d186a65ae069377668fcea47b7, 9fea55b5dd337dcd5c00f4b9c1a09ad2ed5cb7f2c69dc21a7f50f55af0809f89, 06ad76f4b19be8706f98441d926142af824bd2983217f6c2c02201dbb07d0224, 2481e420138bb0bcc52d43a127e76887cc7419ac46e7495f55493d7fccbbec1b, fc76a4046efbaaab93261806f52afcd6cdf88c2784ec2ed7e862089f3d6bbbb8, 8131b5119e869e1ebf7ebce50837f12fa86fa24008d5534b757c23e91e8f401f, 20770419f79550e46c9bdc2dab792cc96792b7ec4dbd8fcc0cedd7c726ae7987, b8baa7b5d0d60070ef78ad846e17198e891093a84a00e3029dad0ffd77c78b7a, 4f6d665fa107ba9d7313ff6bf1527dddf18bcf178ae34c0e573b3afcb52d685f, b14eb9596f91c1625c3df29413fa08ba313a6b9e6d7fb1297fba74761c135568, a908289bef30086660453ab8809af758af3d445ecda4010211282eb067fef3ab

TYPE	VALUE
SHA256	9db1a5e089a0b16b3b9a584cb3e5e55eb68620d0ab6b229cf24d49f32b9391be, 94797cd702cf50fea6d780ab0d94cb2a0aa8ee9aa5332e71479adaa7a5245f27, 8ef658a73b292410dd6a570bc65a0f398e838b5adb141eb9dc81ad124fb46f80, 8d65b1c26285a08ee8cb11aa868984bd37553e2d2a8e5171d2460c32ca89a2e6, bf4178df292e66a5b2eca7a70df0feb76dfb4463cf70d92ee27d71c77af24f2d, 503a6e977c8fb68ffd015b1f882acdd9f90b98612dd41b676ee08ff10c7d0a90, 84d19f243cae6d14a15eced6cadd77f95dc494058f18a463fdcb18c0b382fe0e, ac0151ff4434a5bb31a4ecbfecc0ba66a6deaf344b6a10a9abf7cce7f6eb094a, be98fcecb03b2638632ebb05c1274d276918408b5f6543c6c7f57c80a7802e98, b95c0e0ba3004f72e0da0f618fe230d5053b8ddd402fdb17088e1ad6e605ef4e, 7917138fac54741ec12ed4d79594f399854996b1abd81ae5fb040b14b8ff483c, 208e4ae853feeede9be36b9385aa38e8547d83c979825ba7b9cb53a53c51c513, ea92d80d8b7d8be657eb667347be9e92004a54bf6f124e143744b6efada650cc, 881e7126f65751a41d59e846908246030f834ec03b15c1ef2cae8c4a1098cf15, 8347e8933783cd4129240b96ae5e665cedc5848ce1cbb7d9f58eb97aaa29b108, 18c58f83cf1e51d23eff699bec82fdef08f8a6585f51610bce162c9de25bc549, 60372d900506da46bf83e318f5f8f8c3219dcda3fca977f0172367d6825dfcdb, 1ef241ca77d2de374113db8b9e9bad4133142326683f2c7954bbab6415780dff, ec83fcc94d1fd981d13c7e5f3318671f3c96e677eaa956c7c1df4de2444c326f, 46ff9f7c0e437df7dd6e1c69790c8fc94e65091e9f3cf1f3243c808f1a1e8621, f0eb89b91e787324bb6f4a082fccea951b00f32ae62f31c80d9d83f4c53a0a65, a580c913a1e16d3fe4e7ebf8d155ac9cb08c1fabf831905776aa5ad6a6361f6f,

Patch Details

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-a-new-variant-of-gafgyt-malware

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-vulnerability-in-p660hn-t1a-dsl-cpe

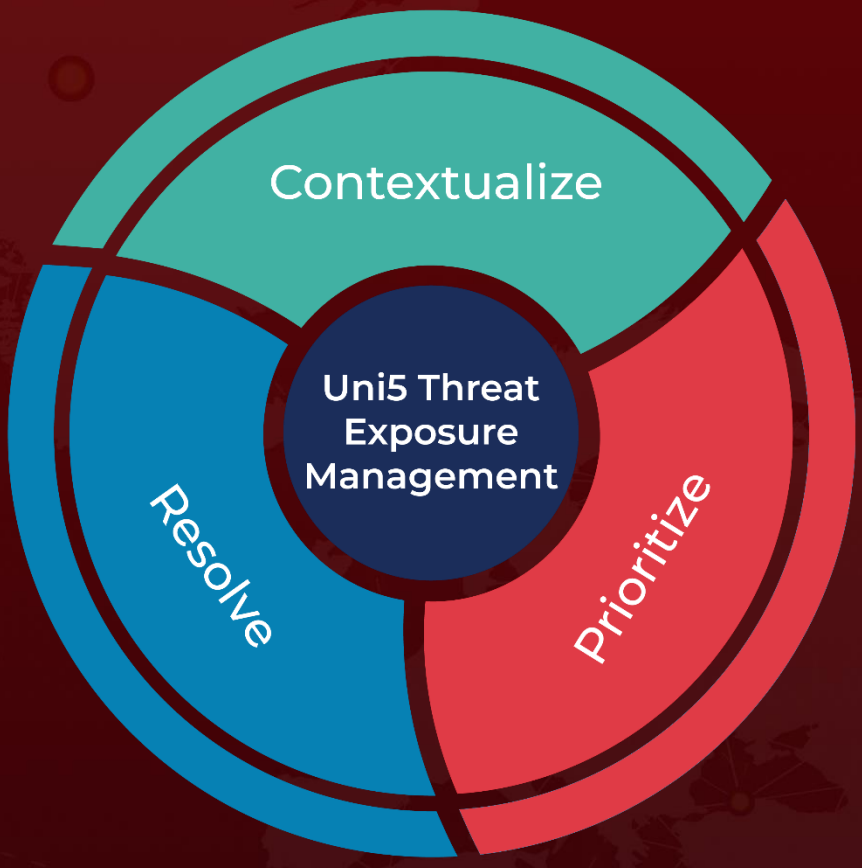
References

https://fortiguard.fortinet.com/outbreak-alert/zyxel-router-command-injection

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

August 11, 2023 • 4:30 AM

More at www.hivepro.com