Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

New Botnet named Zerobot Exploiting Multiple Vulnerabilities

Date of Publication	Admiralty Code	TA Number
December 8, 2022	A1	TA2022289

Summary

First Seen: November 18, 2022
Affected Product: Linux and Windows
Impact: Remote attackers take control of the compromised systems.

⚙ CVE

CVE	NAME	PATCH
CVE-2014-08361	PAC parse integer overflow Vulnerability	✗
CVE-2017-17106	Zivif Webcams Information Disclosure	✗
CVE-2017-17215	RCE vulnerability in Huawei HG532	✓
CVE-2018-12613	Improper Authentication vulnerability in phpMyAdmin	✓
CVE-2020-10987	Command injection vulnerability in Tenda Routers	✗
CVE-2020-25506	Command Injection vulnerability in D-Link DNS-320	✗
CVE-2021-35395	Buffer Overflow vulnerability in Realtek SDK	✓

CVE	NAME	PATCH
CVE-2021-36260	OS command injection vulnerability in Hikvision products	✅
CVE-2021-46422	OS command injection vulnerability in Telesquare SDT-CW3B1 1.1.0	✅
CVE-2022-01388	Authentication Bypass in F5 BIG-IP	✅
CVE-2022-22965	Spring Shell	✅
CVE-2022-25075	Denial of Service (DOS)	✅
CVE-2022-26186	Command injection vulnerability in TOTOLINK	❌
CVE-2022-26210	Command injection vulnerability in TOTOLINK	❌
CVE-2022-30525	OS command injection vulnerability in the CGI program	✅
CVE-2022-34538	Command injection vulnerability in Digital Watchdog cameras	❌
CVE-2022-37061	command injection vulnerability in FLIR AX8 cameras	❌

Vulnerability Details

#1 A new botnet named 'Zerobot' has two variants, both are written in Go programming language, the first variant discovered on 18 Nov 2022, and within a short time on 24 Nov 2022 second variant was developed, and is more sophisticated has number of advanced features, which includes self propagation, self replication and attacks for different protocols.

#2 Zerobot main goal to launch distributed denial of service (DDOS) attacks and gain access on specified targets, which includes D-Link routers, Totolink routers, F5 BIG-IP, Zyxel firewalls and Hikvision cameras. It even targets multiple system architectures and devices including i386, AMD64, ARM, ARM64, MIPS, MIPS64, MIPS64le, MIPSle, PPC64, PPC64le, RISC64, and S390x.

#3 Zerobot uses a number of vulnerabilities to gain access, afterwards, it downloads a script to spread the infection. Later uses WebSocket protocol to communicate with command and control server. Finally it make use of 'anti-kill' module that safeguards against killing or terminating its process.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2014-08361	miniigd SOAP service in Realtek SDK	cpe:2.3:a:realtek:realtek_sdk:*:*:*:*:*:*:*:*	CWD-20
CVE-2017-17106	Zivif PR115-204-P-RS webcams	cpe:2.3:o:zivif:pr115-204-p-rs_firmware:2.3.4.2103:*:*:*:*:*:*:*	CWD-522
CVE-2017-17215	Huawei HG523 router	cpe:2.3:o:huawei:hg532_firmware:-:*:*:*:*:*:*:*	CWE-20
CVE-2018-12613	phpMyAdmin	cpe:2.3:a:phpmyadmin:phpmyadmin:*:*:*:*:*:*:*:*	CWE-287
CVE-2020-10987	Tenda AC15 AC1900 router	cpe:2.3:o:tenda:ac15_firmware:15.03.05.19:*:*:*:*:*:*:*	CWE-78
CVE-2020-25506	D-Link DNS-320 NAS	cpe:2.3:o:dlink:dns-320_firmware:2.06b01:*:*:*:*:*:*:*	CWE-78
CVE-2021-35395	Realtek Jungle SDK	cpe:2.3:a:realtek:realtek_sdk:2.0:*:*:*:*:*:*:*	CWE-119

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2021-36260	Hikvision product	cpe:2.3:h:hikvision:ds-2cvxxx1:*:*:*:*:*:*:*:*	CWE-78
CVE-2021-46422	Telesquare SDT-CW3B1 router	cpe:2.3:o:telesquare:sdt-cs3b1_firmware:1.1.0:*:*:*:*:*:*:*	CWE-78
CVE-2022-01388	F5 BIG-IP	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*	CWE-306
CVE-2022-22965	Spring MVC and Spring WebFlux (Spring4Shell)	cpe:2.3:h:dell:dell_emc_vxrail_appliance:*:*:*:*:*:*:*:*:	CWE-94
CVE-2022-25075	TOTOLink A3000RU router	cpe:2.3:o:totolink:a3000ru_firmware:v5.9c.2280_b20180512:*:*:*:*:*:*:*	CWD-77
CVE-2022-26186	TOTOLink N600R router	cpe:2.3:o:totolink:a810r_firmware:4.1.2cu.5182_b20201026:*:*:*:*:*:*:*	CWE-77
CVE-2022-26210	TOTOLink N600R router	cpe:2.3:o:totolink:a810r_firmware:4.1.2cu.5182_b20201026:*:*:*:*:*:*:*	CWE-77
CVE-2022-30525	Zyxel USG Flex 100(W) firewall	cpe:2.3:h:zyxel_communications_corp:usg_flex_100w:5.00:*:*:*:*:*:*:*	CWE-77
CVE-2022-34538	MEGApix IP cameras	cpe:2.3:o:dw:megapix_firmware:4.2.0.32842:*:*:*:*:*:*:*	CWE-77
CVE-2022-37061	FLIX AX8 thermal sensor cameras	cpe:2.3:o:flir:flir_ax8_firmware:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Security Leaders
Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**T1189** Drive-by Compromise	**T1204** User Execution	**T1588.006** Vulnerabilities
T1587 Develop Capabilities	**TA0040** Impact	**T1499** Endpoint Denial of Service	**TA0002** Execution
T1489 Service Stop	**T1584.002** Compromise Infrastructure: DNS Server	**T1071.004** Application Layer Protocol: DNS	**T1071.001** Application Layer Protocol: Web Protocols
T1049 System Network Connections Discovery	**T1055** Process Injection	**T1105** Ingress Tool Transfer	**T1059** Command and Scripting Interpreter
T1584.005 Compromise Infrastructure: Botnet	**TA0042** Resource Development	**TA0011** Command and Control	**TA0007** Discovery

Patch Links

http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en

https://www.realtek.com/en/cu-1-en/cu-1-taiwan-en

https://tanzu.vmware.com/security/cve-2022-22965

https://github.com/EPhaha/IOT_vuln/blob/main/TOTOLink/A3000RU/README.md

https://gist.github.com/Nwqda/9e16852ab7827dc62b8e44d6180a6899

https://techdocs.f5.com/en-us/bigip-17-0-0/big-ip-release-notes/big-ip-upgrade.html#concept-5278

References

https://www.fortinet.com/blog/threat-research/zerobot-new-go-based-botnet-campaign-targets-multiple-vulnerabilities

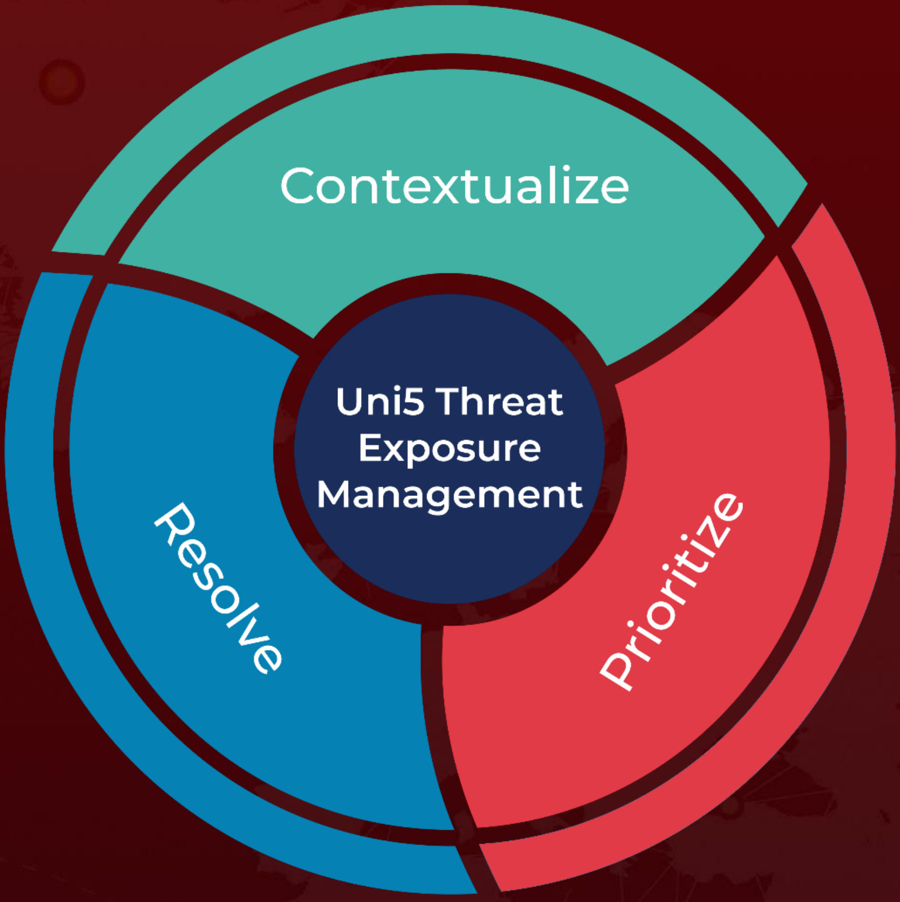
https://www.bleepingcomputer.com/news/security/new-zerobot-malware-has-21-exploits-for-big-ip-zyxel-d-link-devices/

Note: The term "Zerobot" in this advisory refers to a specific type of malware and is not related with the organization zerobot.ai

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**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

December 8, 2022 • 4:30 AM

More at www.hivepro.com