Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

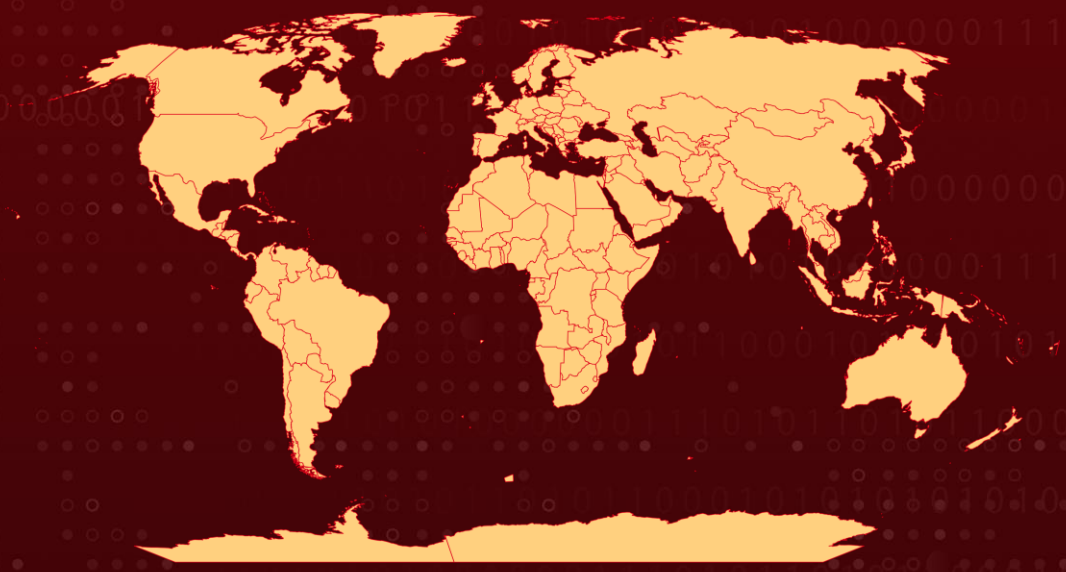
Botnets Actively Exploited Realtek and Cacti Flaws

Date of Publication	Admiralty Code	TA Number
April 6, 2023	A1	TA2023172

Summary

Attack began: January 2023
Malware: ShellBot (aka PerlBot, DDoS Perl IrcBot) and Moobot
Attack Region: Worldwide
Attack: In January and March of this year, there were surges of attacks aimed at exploiting vulnerabilities in Cacti and Realtek. These attacks resulted in the dissemination of ShellBot and Moobot malware.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	CISA KEV	PATCH
CVE-2021-35394	Realtek Jungle SDK Remote Code Execution Vulnerability	Realtek SDK: 2.0 Realtek Jungle SDK: 3.0 - 3.4T-CT Realtek Luna SDK: 1.3.2	✓	✓
CVE-2022-46169	Cacti Command Injection Vulnerability	cacti: before 1.1.19-2.20	✓	✓

Attack Details

#1

ShellBot is a type of malware coded in Perl and utilizes the Internet Relay Chat (IRC) protocol to communicate with the server, also known as PerlBot. Moobot, on the other hand, is a variant of the Mirai botnet that aims to exploit exposed networking devices. CVE-2022-46169 pertains to a severe authentication bypass and command injection flaw that affects Cacti servers, allowing unauthorized users to execute arbitrary code. Furthermore, CVE-2021-35394 involves an arbitrary command injection vulnerability that affects the Realtek Jungle SDK.

#2

In the past, both vulnerabilities have been exploited by several botnet malware, such as Fodcha, RedGoBot, Mirai, Gafgyt, and Mozi. As of September 2022, Moobot has been updated to target multiple D-Link RCE flaws. It currently exploits CVE-2021-35394 and CVE-2022-46169 to infect vulnerable hosts, downloads a script with its configuration, and establishes a connection with the C2 server. In contrast, ShellBot mainly focuses on the Cacti flaw, and its second version has already affected hundreds of victims and features an extensive array of commands.

Recommendations

- To safeguard against Mootbot and ShellBot, it is advised to use strong administrator passwords and apply security updates that address the mentioned vulnerabilities. If the manufacturer of the product no longer provides security updates, it is suggested that you replace it with a newer edition.

- Proactive security measures, such as blocking indicators of compromise (IoCs), are strongly recommended due to the serious security impact of the aforementioned vulnerabilities, which can result in remote code execution. It is therefore highly advised that patches and upgrades be applied as soon as possible. Additionally, increasing security posture requires the adoption of preventive and detecting strategies, such as setting up a firewall rule to restrict inbound and outbound traffic to and from the attacker's IP address.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0042** Resource Development
T1003 OS Credential Dumping	**T1070** Indicator Removal	**T1071** Application Layer Protocol	**T1082** System Information Discovery
T1095 Non-Application Layer Protocol	**T1110** Brute Force	**T1190** Exploit Public-Facing Application	**T1518** Software Discovery
T1518.001 Security Software Discovery	**T1543** Create or Modify System Process	**T1543.002** Systemd Service	**T1571** Non-Standard Port
T1583 Acquire Infrastructure	**T1583.005** Botnet		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	104[.]244[.]76[.]105 156[.]224[.]24[.]249 206[.]217[.]205[.]24 199[.]195[.]250[.]172 80[.]68[.]196[.]6 85[.]239[.]33[.]32 46[.]101[.]183[.]162 49[.]212[.]234[.]206:3303 198[.]98[.]61[.]106:8080
Domains	apid[.]mutoujs[.]xyz troon[.]dns[.]army botnet[.]goelites[.]cc j[.]xnyidc[.]top www[.]xiaojue[.]cyou bot[.]layer7[.]top juice[.]baselinux[.]net:6667

TYPE	VALUE
SHA256	bc1ded2f3a9fc50614a159b3971a26868e6a5b09a6f6ba65d6bee1b05335e69b,55048b3df95d4dbb681be32cfe6c9e4a128045917c49da9ff1c30723debc1854,661f0fb1cf928c40333eaefc86522ddc74c7b96a8e32b93ed8153b8244d66721,d3b13f71e7637d7118ac3e170d33b3bbb15814357e21fa3318b4bf7ecbe6dc7b,0d4be7af347f2cb80dcd71cd94f1f39a6f3dbe71765d824bb0d66c11b8759cd7,e2075d6b723d7daf2303af31e3970ed79d435e52b4338ee63499c4644332ea10,3dbea4436ef3e00dcfb73608164e3d1ded9434f8ee1679cd3a790e22c91cbe11,455314a186b4a9a1788e2acb85a9b6b34fb0a7700d0decc6de056030fea543df,cd47c9db5e3ec59221361ca7459bb12a5a84014c1f8aa2e2bdad07ccb37a4e29,9144c4768b457fb5384bc807d9e992671c25dbefe9d2781672c018e1b4d8c36a,979bf642f67d5df2e8fa664c0bdecbc2954c9ced44f47122c71ad5f71a52aa0d,e2ff90f5bdf51da577be88266cc9dc8be48f1776af46949dcdd2d54e4c84449f,0cb77fabcef38d5ec4e1e64945bac8c33ea8e97346a3140e67ec30eecedc9ea0,0cd6a246eb6933bf5ac8639d8972e2c80dcdb7723a15435a914cf6b5bd30af4c,cf1b136558e7b5faf6bfce3b460afed06e613ca6747257273571399d106dea2b,175b536d5c825b78bd2567b836bb18046928f33f7ae1865afb66a4fe064ebb81,cdf1c2610bde8ae870bc083d06fb00ba1c3441c075fc6c26e9cc9f93c9a3703f,903c340da7c6ef32b2e3098389748fc5d94e88e61bfeea8a67313327f021fb9f,33aa8e731eca7ba051626845541f91fad6f69862aa1deaea7b80a15dae8d67bf,f473597e5fda9051522a52c78965d0eb050ff2971cfce8d359618e1c136ad77b,de5e60ab541838c4c3cb0bfd0733417f2fe4a19bac08683391022cdaabe263de,565d09c8fc9f712b82eae45a39029ac996904564cc08dae6306678081087e933,c33c66e7a161718da4535b34078edb04600c5a06eb1e05fe514a5ad5ac149594,e356ba8fe6ae21fbbba785ade3220a666e3fae947c68093e05b01f0c3f98e15f,7e4dadf93fbb7a01b55eadacbb40ae8d5e95f5b9592e55f0fb2340d89fc78f17,ae2c71e3e177721c336f76946d24b95512accf677c87e829a31b315d56624df3,e1366976365db1f2bffdc37d4e64e12f883f9a20e02b12d52b6a1b346b8f0692,abb3d04a081ee199cfb5687361fbbca3fa2012f588832e05de0e21874f162afd,5f0f2b2e3e839e50631b89cc2e9d980b337db417cab51f21beb0a56043297a6f,7d2c0cba18d51ed84e7a888d56dbcb5e73c1d076ed5f8e5db2528f826601b2cc,9a067e32dd6c25053c302de7caf61cdc0f3982289eb91d06c449fe08a47fc6d3,6804cebbf837d7c5559519c364cc0b20c4f9b514c74039321bc69bcfdbfb5e93,947675c8b2a65bf9b38f4d3d15d108e0826f570086c6a758d3e02be9315da1cd,c05cf5b2c94edd15c40db1ce52f97bdc09ec61e78386c8878b15515cbde99528,47ac3a2c51fc64479ceff1e842a414bc11dc59b9dcdbd3dd1bf011e243f91ffa,0c67234ce88958c9319ca9a8f8fdc4b4869013687151532450 9ac956704f1373,b7d62d1a145ddda241e624ef94ab31fcca1a13f79e130d0a704586e35745282a

Patch Links

https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf

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

https://github.com/Cacti/cacti/commit/7f0e16312dd5ce20f93744ef8b9c3b0f1ece2216

https://github.com/Cacti/cacti/commit/a8d59e8fa5f0054aa9c6981b1cbe30ef0e2a0ec9

https://github.com/Cacti/cacti/commit/b43f13ae7f1e6bfe4e8e56a80a7cd867cf2db52b

https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf

References

https://www.fortinet.com/blog/threat-research/moobot-strikes-again-targeting-cacti-and-realtek-vulnerabilities

https://www.hivepro.com/the-vulnerability-discovered-in-the-cacti-open-source-rrd-tool/

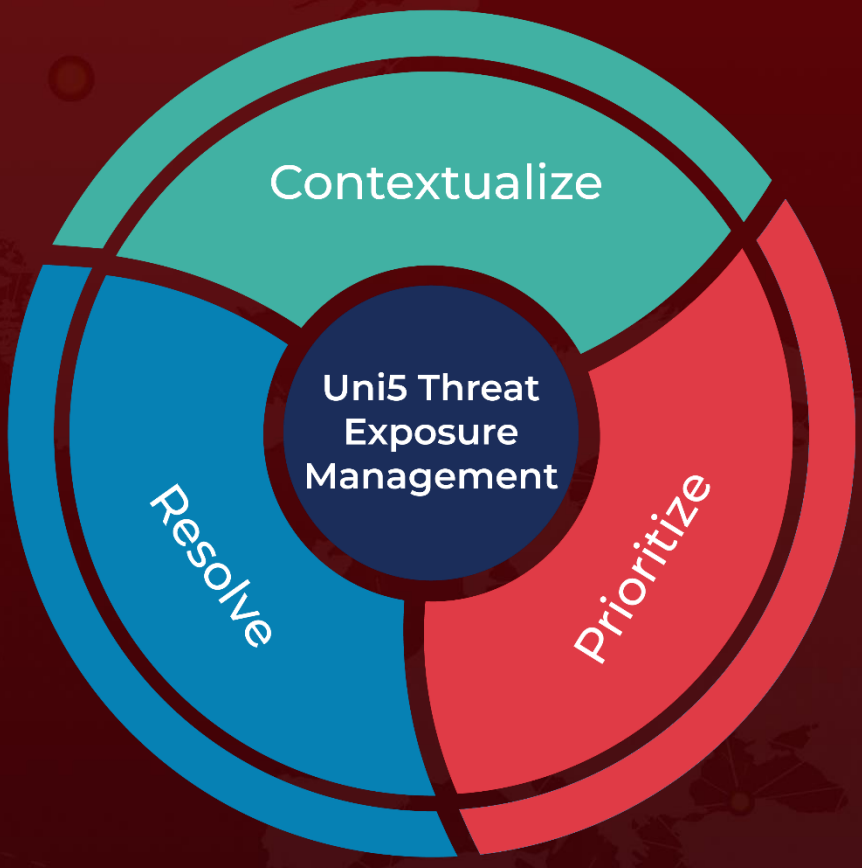
https://www.hivepro.com/shellbot-malware-targets-mismanaged-linux-servers/

https://unit42.paloaltonetworks.com/realtek-sdk-vulnerability/

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

April 6, 2023 . 6:46 AM

More at www.hivepro.com