Recent Attack Uses Vulnerability on Confluence Server

fortinet.com/blog/threat-research/recent-attack-uses-vulnerability-on-confluence-server

October 21, 2021

FortiGuard Labs Threat Research Report

Affected platforms: Atlassian's Confluence
Impacted parties: Confluence Server or Data Center instance
Impact: An OGNL injection vulnerability exists that would allow an unauthenticated user to execute arbitrary code
Severity level: Critical

Introduction of CVE-2021-26084

In August 2021, Atlassian published a security advisory about CVE-2021-26084 that could enable a threat actor to run arbitrary code on unpatched Confluence Server and Data Center instances. FortiGuard Labs analyzed the situation and published a Threat Signal with relevant information. After releasing the advisory, there occur massive scanning and proof-of-

concept exploit code in public. We also collect a lot attacking traffic. In this blog we will analyze the payloads leveraging this vulnerability, deep dive into the attack and summarize the IOCs for these suspicious activities that may hint the network was affected by CVE-2021-26084.

Overview of CVE-2021-26084 Incidents

In September, we observed numerous threat actors targeting this vulnerability whose goal was to download a malicious payload that would install a backdoor or miner in a user's network. These threats include Cryptojacking, Setag backdoor, Fileless attack that uses PowerShell in a system to execute shell without file dropped and Muhstik botnet; we will elaborate each of them in this analysis.

Although there are different attack vectors for this vulnerability, all of these attacks are targeting the parameter "queryString" which is shown in following packet capture:

Fileless attack leverage CVE-2021-26084

Cryptojacking

After exploiting CVE-2021-26084, it downloads init.sh from 86.105.195[.]120. The shell is a crypto miner that includes following tasks:

1. Delete syslog
2. Change commonly used command
3. Stop aliyun services and apparmor
4. Set the path for miner execution file (zzh) and itself but rename as newinit.sh
5. Kill all other miner processes
6. Use crontab to establish persistence
7. Get scanning shell (is.sh)
8. Clean the trace

Payload Exploits CVE-2021-26084

Inti.sh

In the scanning shell, it will try to download a scanning tool, like Masscan, Pnscan, etc, which can be used to scan and survey IPv4 TCP network in order to discover live host to proceed the spreading. The downloader path is shown as below. It also downloads a shell that defines specific steps for the scan. First, get the login brute force tool hxx (md5: f0551696774f66ad3485445d9e3f7214) and account/password list ps (md5: a43ad8a740081f0b5a89e219fe8475a3), then scan the subnet belong to private network (172.16.0.0/12, 192.168.0.0/16, 10.0.0.0/8). This is to allow the malware to login into more devices in victim's intranet and spread miner script (init.sh).

Downloader path in is.sh

Scannng steps in rs.sh

The entire workflow can be seen below.

Confluence server

Setag

The following exploit traffic was observed from IP address 86.105.195.154 (AS 3164 Astimp IT Solution SRL). Setag, also known as BillGates or Ganiw, belongs to a well-known malware family that targets server via 1 day vulnerability. It mainly uses UDP/SYN/ICMP/DNS floods to conduct DDoS attack. But it also has various command can check its own status or control their victims. The command for dos attack or controlling their victims can be seen in following rawdata:

Syna

Fileless Attack

The observed packet is from 141.98.83.139 (AS 209588 Flyservers S.A.) and the main payload is b64 encoded. The decoded data is as follow:

First layer decoded data

We can see that the payload is constructed and executed via PowerShell. The final execution will set “WindowStyle” to hidden and “CreateNoWindow” to True, which is to put itself out of sight. We decoded those data in the middle and replace {0} and {1} with “=” and “P”, then 2nd layer payload data

Second layer payload data

It defined two functions, and one variable that contain the main exploit code. After converting the code in $sG, it will use VirtualAlloc to reserve a part of memory. Then it uses CreateThread to invoke the malicious code. So what exactly $sG is? After b64 decoding, we get about 570 bytes binary data as below:

570 bytes binary data

To dive deep in to this, we have to check this binary by IDA. Following the first call into loc_D6, it puts ws2_32 and move edx, 726774ch, and this is the hash value of LoadLibrary function, the detail code is as below:

The hash value of LoadLibrary function

It is a reverse shell meterpreter shellcode that connects to exploit source 141.98.83[.]139 via tcp port 23733. Since the port now is closed, we only managed to capture the following packets. But the entire attack process only leveraged PowerShell to decode layer by layer, and uses hidden window style to hide itself. And finally, create a thread to achieve the reverse shell. Not a single file is dropped in the entire attack, which is known as fileless attack.

Muhstik

By exploiting CVE-2021-26084, it downloads conf2 from 149.28.85[.]17. The file will deploy and execute dk86 from 188.166.137[.]241 and ldm script. The attack scenario afterward is analyzed in this article, but we observed a different server IP and more attack source IP which is intended to spread conf2 of Muhstik.

Different conf2 downloader

Conclusion

We have been tracking this vulnerability for weeks and observing massive threat exploitation targeting Atlassian Confluence. Although the patch for CVE-2021-26084 is already released, public attacks are still undergoing. In this post, we gave detail of those attacks and illustrate how they using the payload to deliver malware, users should upgrade the system immediately and also apply Fortiguard protection to avoid the threat probing.

Fortinet Protections

For vulnerability CVE-2021-26084, Fortinet already release IPS signature Atlassian.Confluence.CVE-2021-26084.Remote.Code.Execution for it to proactive protect our customer. For payloads described are detected and blocked by the FortiGuard AntiVirus.

The downloading URLs and attacker's IP addresses have been rated as "Malicious Websites" by the FortiGuard Web Filtering service.

IOC

Value	Item
86.105.195.154	Cryptojacking expolit source IP address
86.105.195.120	Cryptojacking dropper hosting IP address

911e417b9bc8689a3eed828f0b39f579	hxxp://86.105.195.120/cleanfda/init.sh hxxp://86.105.195.120/cleanfda/newinit.sh
75259ee2db52d038efea5f939f68f122	hxxp://86.105.195.120/cleanfda/zzh
4a7bf7f013cc2297d62627b2b78c5b0b	hxxp://86.105.195.120/cleanfda/is.sh
8cc2b831e29dc9f4832a162e9f425649	hxxp://86.105.195.120/cleanfda/rs.sh
2.57.33.59	Setag expolit source IP address
209.141.50.210	Setag dropper hosting IP address
a8eb59396d698bda5840c8b73c34a03b	hxxp://209.141.50.210/syna
141.98.83.139	Fileless attack expolit source IP address
1b8a7954b9630be2e0dd186a4fc6a32a	2nd layer payload data
bf8a7b199f3293852c7f2b3578e8c0ae	Binary shellcode
98.239.93.20 87.106.194.46 51.75.195.137 34.247.148.227 121.196.25.170 221.168.37.77 122.9.48.250 18.182.153.49	Muhstik exploit source IP address
149.28.85.17	Conf2 dropper hosting IP address
6078c8a0c32f4e634f2952e3ebac2430	hxxp://149.28.85.17/conf2

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda (TAA), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program. Learn more about FortiGuard Labs global threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.