



RCE in Splunk Enterprise

 for SOC Analysts

CVE-2023-46214

TABLE OF CONTENTS

01

Alert

04

Detection

05

Analysis

13

Containment

14

Appendix

Author: Muhammet Donmez

Alert

Looking at the reason that triggered the alert, it was seen that an attempt was made to upload the Malicious XSLT file, which enables RCE to run on Splunk Enterprise. The alarm violated the SOC239 - Remote Code Execution Detected in Splunk Enterprise rule.

★ Splunk App for Lookup File Editing RCE via User XSLT	
EventID :	201
Event Time :	Nov, 21, 2023, 12:24 PM
Rule :	SOC239 - Remote Code Execution Detected in Splunk Enterprise
Level :	Security Analyst
Source IP Address :	180.101.88.240
Destination IP Address :	172.16.20.13
Hostname :	Splunk Enterprise
HTTP Request Method :	POST
Requested URL :	http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xml
Trigger File Path :	/opt/splunk/var/run/splunk/dispatch/1700556926.3/shell.xml
Alert Trigger Reason :	Detected a malicious XSLT upload in Splunk Enterprise with the potential to trigger remote code execution.
Device Action :	Allowed
File (Password:infected) :	Download

First, this alert should be verified by checking the existing logs, then the source of this traffic should be investigated and it should be confirmed whether it is legal traffic.

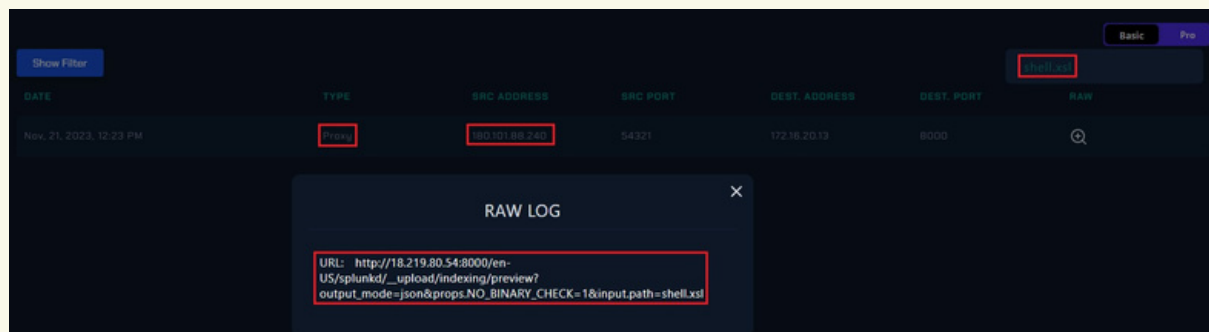


Detection

Verify

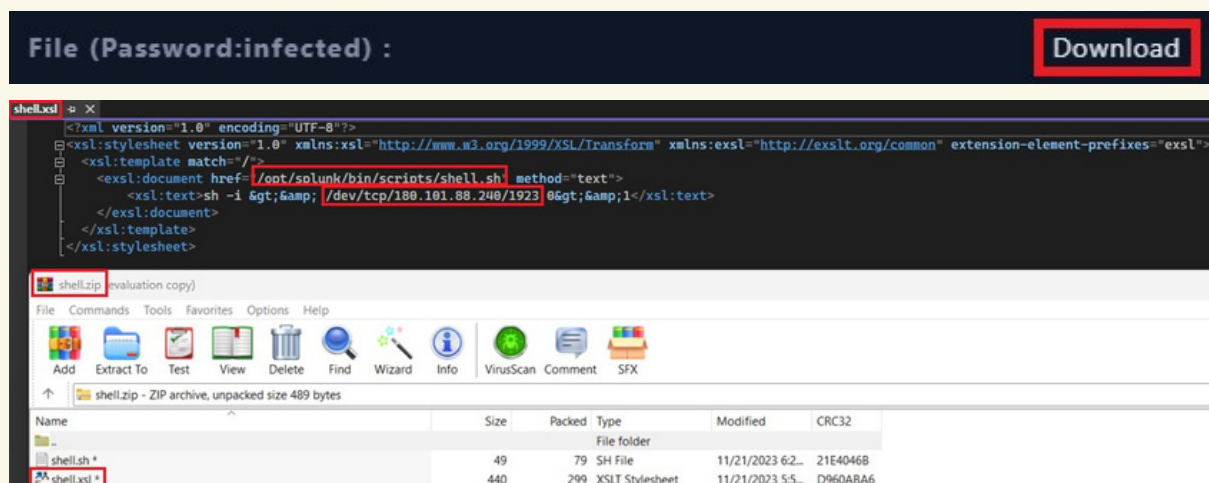
The alarm was triggered as a result of trying to upload the file named "shell.xml" on Splunk in the request coming to the system. Below is the request that triggered the alarm. The relevant request can be searched and confirmed on Log Management.

RequestURL: http[://]3.133.116.124:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xml



As can be seen above, the relevant request came at "12:23 PM". It was seen that the relevant request came from the IP address "180.101.88.240" located in China. As a result of the investigations carried out so far, it has been confirmed that there was an attempt to upload files to the system. Therefore the corresponding alarm is True Positive. However, in order to make a clear decision, it is necessary to examine the content of the file being tried to be uploaded.

Relevant files have been shared for download in detail of the alarm.



Analysis

Reputation Check

While uploading the file, the reputation of "180.101.88.240" seen in the Source IP should be checked.

180.101.88.240 was found in our database!

This IP was reported **12,872** times. Confidence of Abuse is **100%**: ?

100%

ISP	ChinaNet Jiangsu Province Network
Usage Type	Data Center/Web Hosting/Transit
Domain Name	chinatelecom.com.cn
Country	China
City	Suzhou, Jiangsu

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 180.101.88.240

WHOIS 180.101.88.240

IP Abuse Reports for **180.101.88.240**

This IP address has been reported a total of **12,872** times from 65 distinct sources. 180.101.88.240 was first reported on August 17th 2023, and the most recent report was 3 minutes ago.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
Abuse Reporting	2023-11-22 09:44:33 (3 minutes ago)	Nov 22 09:43:23 Server-Eygelsho sshd[193982]: Failed password for root from 180.101.88.240 port 1402 ... show more	<div>Brute-Force</div> <div>SSH</div>
Valea	2023-11-22 09:41:33 (6 minutes ago)	Nov 22 10:41:27 dockerhost sshd[2255944]: Failed password for root from 180.101.88.240 port 62928 ss ... show more	<div>Brute-Force</div> <div>SSH</div>
SIT	2023-11-22 09:40:43 (6 minutes ago)	Nov 22 10:39:27 cloud01 sshd[3150313]: Failed password for root from 180.101.88.240 port 10441 ssh2< ... show more	<div>Brute-Force</div> <div>SSH</div>
devmoon.de	2023-11-22 09:22:45 (24 minutes ago)	Nov 22 10:21:25 docker-01 sshd[799116]: Failed password for root from 180.101.88.240 port 19079 ssh2 ... show more	<div>Brute-Force</div> <div>SSH</div>
Abuse Reporting	2023-11-22 09:20:23 (27 minutes ago)	Nov 22 09:19:09 Server-Eygelsho sshd[193016]: Failed password for root from 180.101.88.240 port 2131 ... show more	<div>Brute-Force</div> <div>SSH</div>

<https://www.abuseipdb.com/check/180.101.88.240>

13

/ 88

13 security vendors flagged this IP address as malicious

Similar

Graph

API

180.101.88.240 (180.101.88.0/21)

CN

Last Analysis Date 3 days ago

AS 4134 (Chinanet)

Community Score

DETECTION

DETAILS

RELATIONS

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Phishing
CRDF	Malicious	Criminal IP	Malicious
CrowdSec	Malicious	CyRadar	Malicious
ESTsecurity	Malicious	Fortinet	Malware
G-Data	Phishing	GreenSnow	Malicious
IPsum	Malicious	Lionic	Malicious
SOCRadar	Malicious	AlphaSOC	Suspicious
ArcSight Threat Intelligence	Suspicious	Abusix	Clean

<https://www.virustotal.com/gui/ip-address/180.101.88.240>

The relevant IP is located in China and belongs to the hosting companies. When checks are made on both AbuseIPDB and Virus Total for the IP 180.101.88.240, it is seen that the relevant IP is reported by different sources in categories such as brute force, phishing, and hacking.



Initial Access

Before starting the analysis, the details of the RCE that the attacker tried on the system should be investigated. Which vulnerability on the system should the relevant RCE arise from? If this question is understood, investigations will become easier. There is a detail shared as a real-world example in the alert details.

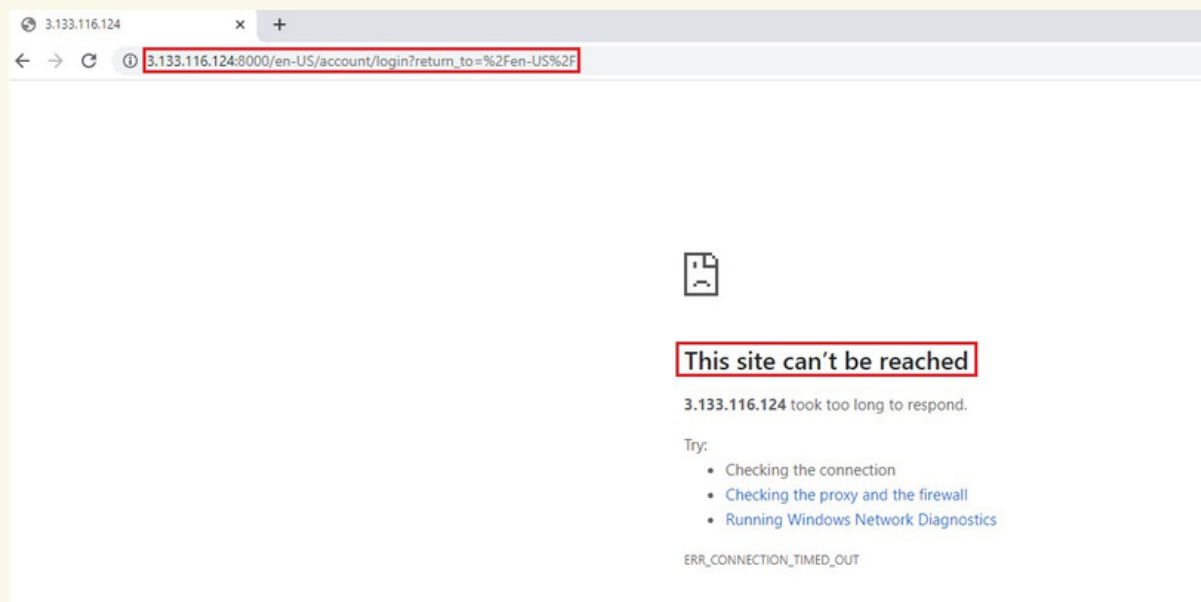
★ Splunk App for Lookup File Editing RCE via User XSLT	
EventID :	201
Event Time :	Nov. 21, 2023, 12:24 PM
Rule :	SOC239 - Remote Code Execution Detected in Splunk Enterprise
Level :	Security Analyst
Source IP Address :	180.101.88.240
Destination IP Address :	172.16.20.13
Hostname :	Splunk Enterprise
HTTP Request Method :	POST
Requested URL :	http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xsl
Trigger File Path :	/opt/splunk/var/run/splunk/dispatch/1700556926.3/shell.xsl
Alert Trigger Reason :	Detected a malicious XSLT upload in Splunk Enterprise with the potential to trigger remote code execution.
Device Action :	Allowed
File (Password:infected) :	Download

When we search for "Splunk App for Lookup File Editing RCE via User XSLT" on Google, we come across the CVE-2023-46214 vulnerability. In the details of the relevant vulnerability, it was shared that in vulnerable versions, attackers can upload the malicious "XSLT" file to the target systems, which will allow remote code execution (RCE) on the target system.

Product	Version	component	Affected Version	FixVersion
Splunk Enterprise	9.0	Splunk Web	9.0.0 to 9.0.6	9.0.7
Splunk Enterprise	9.1	Splunk Web	9.1.0 to 9.1.1	9.1.2
Splunk Cloud	-	Splunk Web	Versions below 9.1.2308	9.1.2308

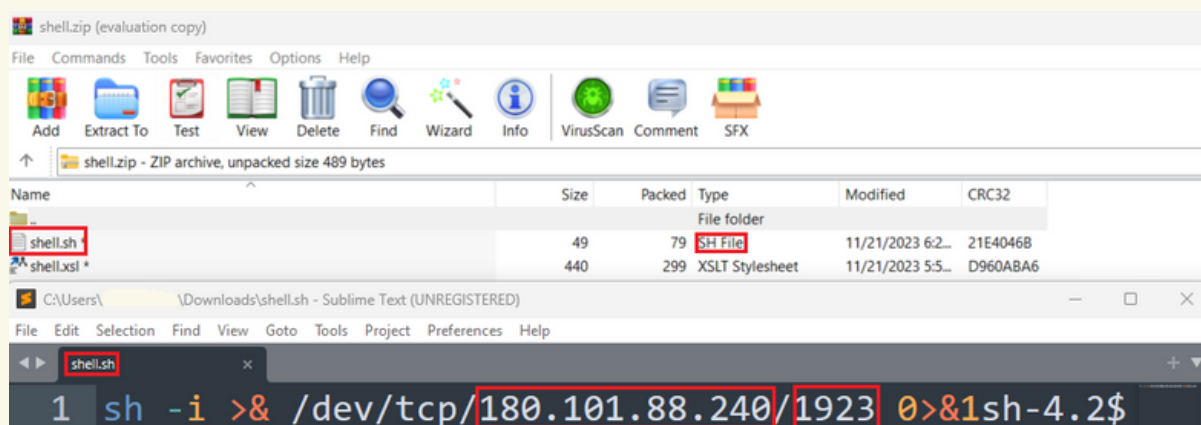
Source: <https://advisory.splunk.com/advisories/SVD-2023-1104>

When a detailed POC examination was performed for the relevant vulnerability, it was seen that the attacker needed a few prerequisites to exploit the relevant vulnerability in the target system. The first and important prerequisite is accessibility to the target system. So, as here, the target system must have access to 3.133.116.124 (Splunk IP) Remote or the information must have been compromised by someone who has accessed it. For example, let access to Splunk remote be disabled. However, remote access to the system should be possible with VPN. The VPN information of the person(s) accessing here must be leaked. So here it is less likely that the target system is open to remote. To test this, access can be attempted via port 8000 of the relevant IP. As a result of the relevant control, access to Splunk could not be achieved, as can be seen below.



It is understood from here that access to the target system was achieved through other means. The system was accessed with the credentials of others (3rd party company employees), which is one of the most commonly used methods by attackers. Thus, "Trusted Relationship(T1199)" can be said for access initial. In addition, a second initial access technique can be called "Exploit Public-Facing Application". Because the attacker exploited the vulnerability in Splunk to gain access to the system.

The second important point to exploit the vulnerability is the credential information of the user who is authorized to log in to the target system. After the attacker logs into the target system with the Python code he will run, he leaves "shell.sh" in the "/opt/splunk/bin/scripts/" file path. The content of the relevant file is among the files shared in the alert details and can be viewed from there.

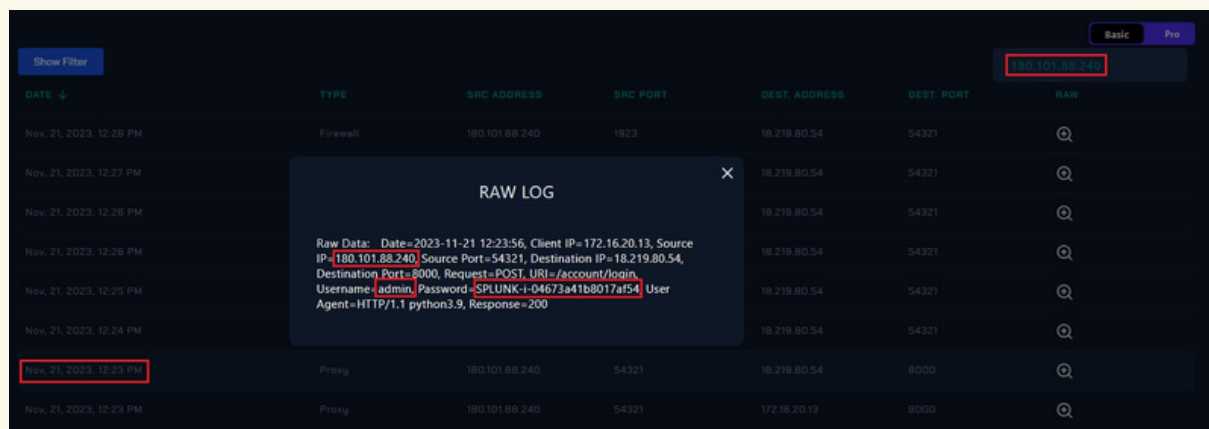


The above file is apparently a Bash reverse shell command. This command is used to create a shell on a target system and direct that shell as a reverse connection to the specified IP address and port number. Creates a TCP connection using Bash's

/dev/tcp feature. Creates a reverse connection with the specified IP address (180[.]101.88.240) and port number (1923).

The analysis so far has been on files shared on alert. It is understood from these files that the attacker intended to receive a reverse shell on the target system. These activities should be confirmed by checking the logs in Log Management.

All traffic of IP “180[.]101.88.240” trying to upload “shell.xsl” to Splunk should be examined. As a result of the relevant search, proxy and firewall logs are seen on Log Management. Logs should be sorted by time and examined in detail. The first proxy log is the log of file uploading to the system. Details can be seen below in the second proxy log. It is seen that the attacker sent an authentication request to the system via the 8000 port, as can be seen in the username and password log.

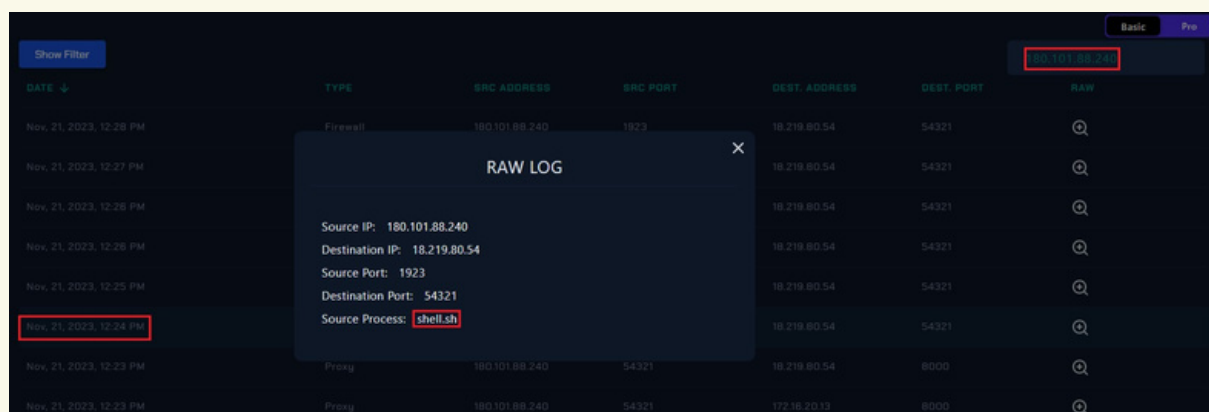


The screenshot shows the Splunk Log Management interface. A table lists logs with columns: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST ADDRESS, DEST PORT, and RAW. A modal window titled 'RAW LOG' is open, displaying the raw data for a selected log entry. The raw data includes: Date=2023-11-21 12:23:56, Client IP=172.16.20.13, Source IP=180.101.88.240, Source Port=54321, Destination IP=18.219.80.54, Destination Port=8000, Request=POST, URI=/account/login, Username=admin, Password=SPLUNK-i-04673a41b8017af54, User Agent=HTTP/1.1 python3.9, Response=200. The IP address 180.101.88.240 is highlighted in the search bar and the raw data.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST ADDRESS	DEST PORT	RAW
Nov. 21, 2023, 12:28 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov. 21, 2023, 12:27 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:25 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:24 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

The details of the proxy log show the user and password information used by the attacker to log in to the target system.

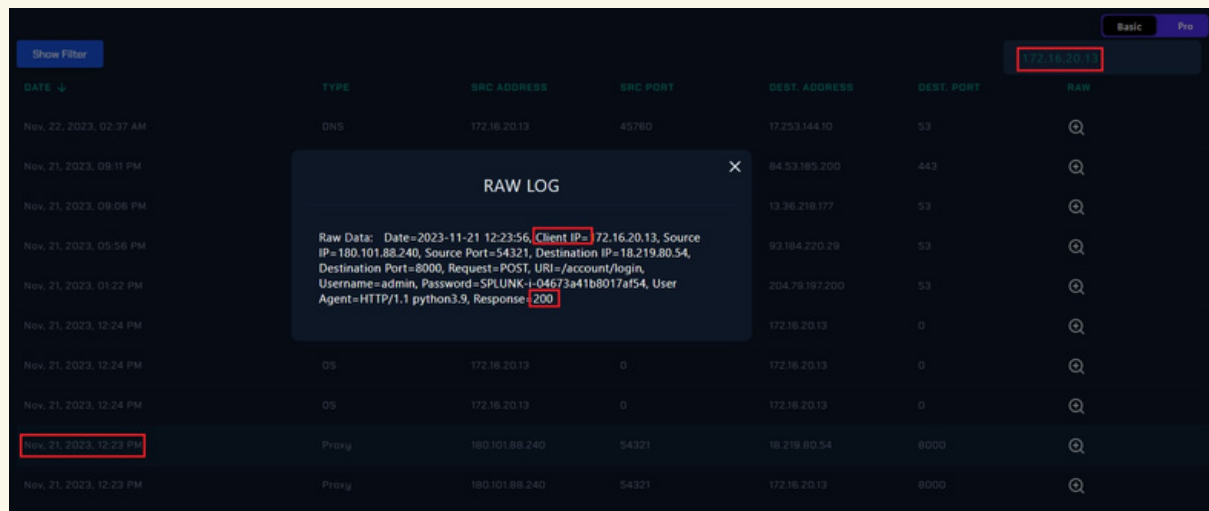
When all logs of the Attacker IP are examined on Log Management, it is thought that a reverse shell connection was established as of 12:24 PM. Because a lot of Firewall traffic is seen, with Source IP being “180.101.88.240”, source port being “1923” and Destination IP being “18.219.80.54 (Splunk IP)”.



The screenshot shows the Splunk Log Management interface. A table lists logs with columns: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST ADDRESS, DEST PORT, and RAW. A modal window titled 'RAW LOG' is open, displaying the raw data for a selected log entry. The raw data includes: Source IP: 180.101.88.240, Destination IP: 18.219.80.54, Source Port: 1923, Destination Port: 54321, Source Process: shell.sh. The IP address 180.101.88.240 is highlighted in the search bar and the raw data.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST ADDRESS	DEST PORT	RAW
Nov. 21, 2023, 12:28 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov. 21, 2023, 12:27 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:25 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:24 PM				18.219.80.54	54321	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

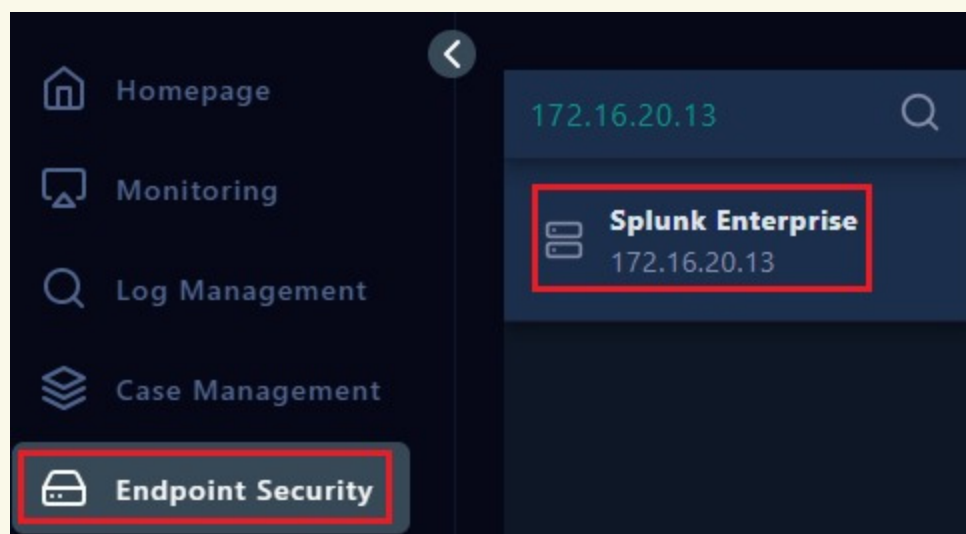
In the alarm details, "172.16.20.13" is seen as the destination IP. If the IP 18.219.80.54 belongs to Splunk, what is this IP? This IP is Splunk's local IP. In the details of the proxy logs, it is seen as the client for this IP.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.10	53	
Nov. 21, 2023, 09:11 PM				84.53.185.200	443	
Nov. 21, 2023, 09:06 PM				13.36.218.177	53	
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

RAW LOG
Raw Data: Date=2023-11-21 12:23:56, Client IP= 172.16.20.13, Source IP= 180.101.88.240, Source Port= 54321, Destination IP= 18.219.80.54, Destination Port= 8000, Request= POST, URI= /account/login, Username= admin, Password= SPLUNK-i-04673a41b8017af54, User Agent= HTTP/1.1 python3.9, Response= 200

The relevant IP can be searched in Endpoint Security to confirm. As a result, it appears that the relevant IP belongs to the "Splunk Enterprise" host.



While examining Log Management, it is necessary to search according to the relevant local IP. Because the attacker's behavior after receiving a Reverse Shell on the target system should also be examined. For this reason, it is expected that the relevant logs appear on local IP.

Show Filter						
DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.10	53	🔍
Nov. 21, 2023, 09:11 PM	Firewall	172.16.20.13	64775	84.53.185.200	443	🔍
Nov. 21, 2023, 09:06 PM				13.36.218.177	53	🔍
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	🔍
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	🔍
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	🔍
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	🔍
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	🔍
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	🔍
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	🔍

RAW LOG

Source IP: 172.16.20.13
 Destination IP: 172.16.20.13
 Destination Port: 0
 Message: session opened for user admin(uid=0) by (uid=0)

As can be seen above, when searching for IP 172.16.20.13, there are OS, DNS and Firewall logs after the proxy logs. Continuing the analysis by time, it is seen that the attacker logged in with “admin” at 12:24 PM. In the following OS log, it is seen that the attacker added users to gain permanence on the system.

Show Filter						
DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.10	53	🔍
Nov. 21, 2023, 09:11 PM	Firewall	172.16.20.13	64775	84.53.185.200	443	🔍
Nov. 21, 2023, 09:06 PM				13.36.218.177	53	🔍
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	🔍
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	🔍
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	🔍
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	🔍
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	🔍
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	🔍
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	🔍

RAW LOG

Username: admin
 Source Process Name: bash
 Target Process Name: useradd
 Target Process Command Line: useradd -m analyst

Add User

Show Filter						
DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.10	53	🔍
Nov. 21, 2023, 09:11 PM	Firewall	172.16.20.13	64775	84.53.185.200	443	🔍
Nov. 21, 2023, 09:06 PM				13.36.218.177	53	🔍
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	🔍
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	🔍
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	🔍
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	🔍
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	🔍
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	🔍
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	🔍

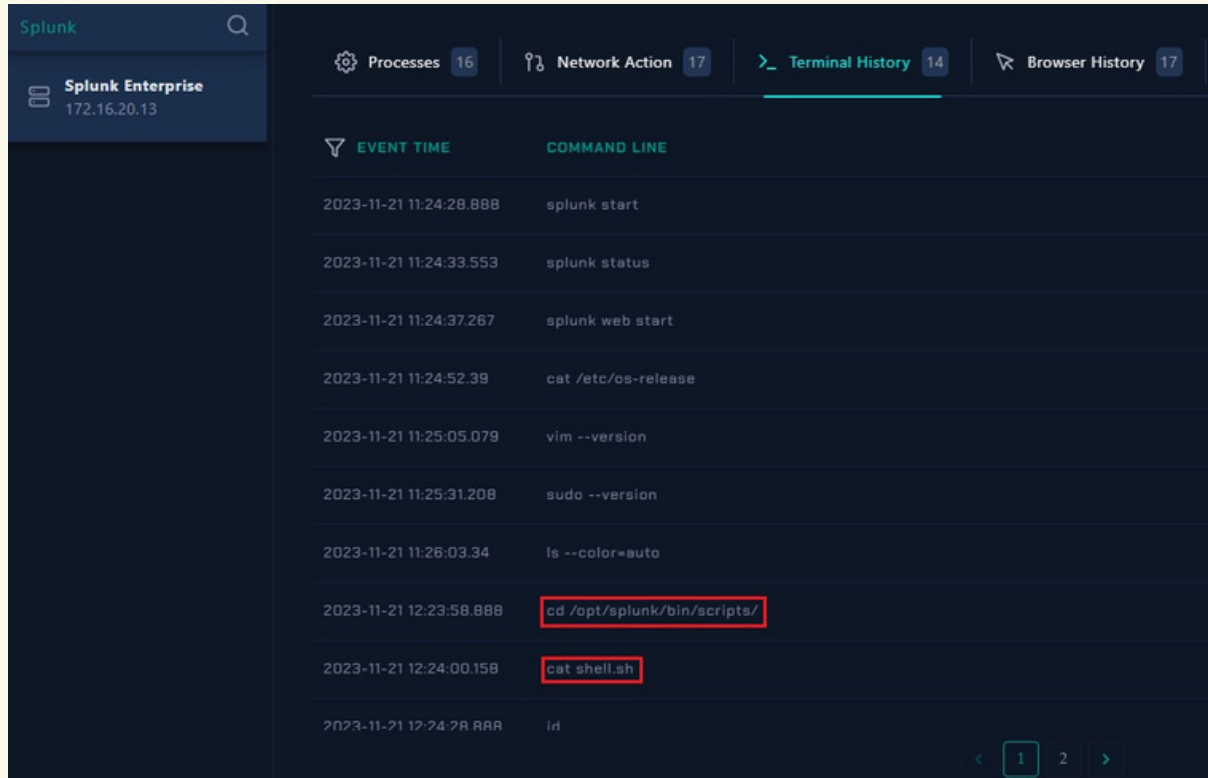
RAW LOG

Username: admin
 Source Process Name: bash
 Target Process Name: passwd
 Target Process Command Line: passwd analyst

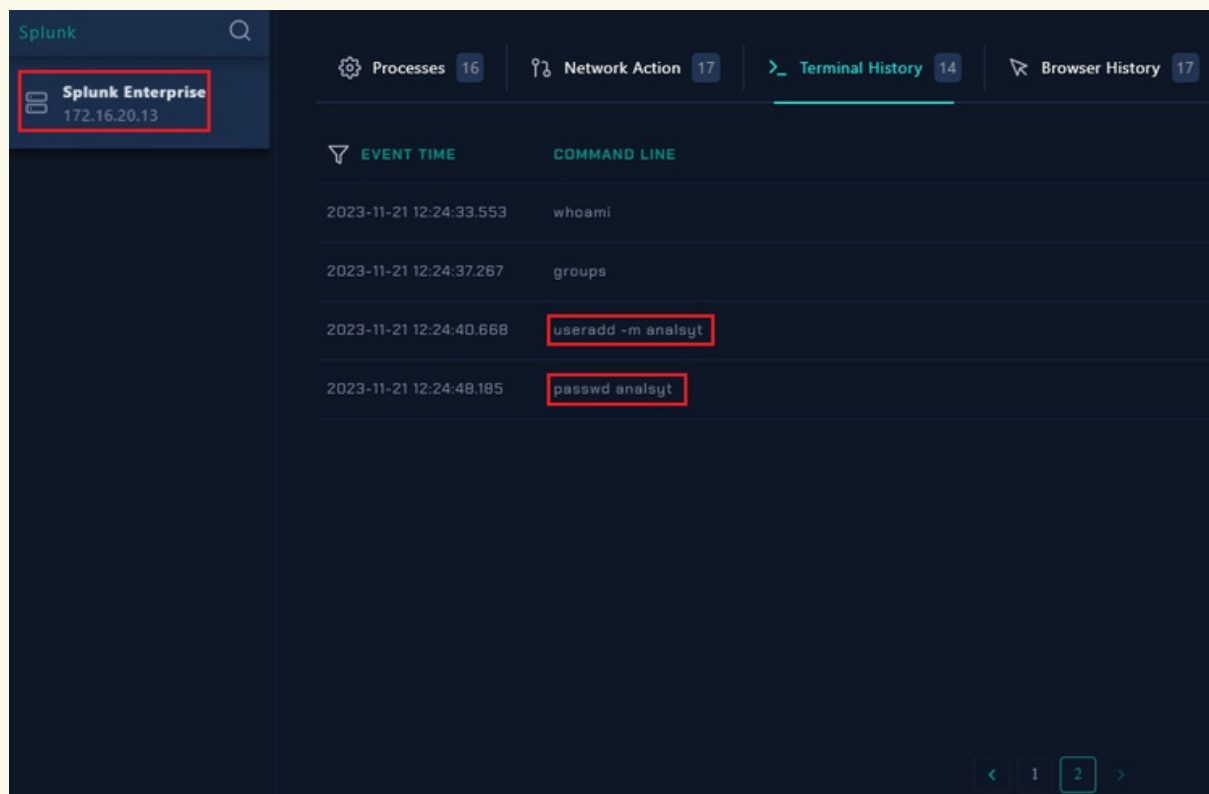
Password Assignment

There is no suspicious situation in the subsequent DNS and Firewall logs of the relevant IP.

The last thing to check is the terminal history of the relevant host. The purpose here is to detect the activities of the attacker on the target system after gaining access to the system. For this, you must go to Endpoint Security.



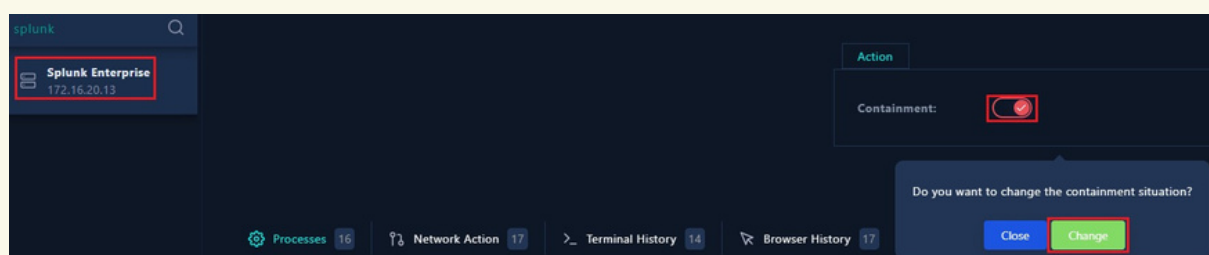
Splunk Enterprise 172.16.20.13		Processes 16	Network Action 17	Terminal History 14	Browser History 17
EVENT TIME	COMMAND LINE				
2023-11-21 11:24:28.888	splunk start				
2023-11-21 11:24:33.553	splunk status				
2023-11-21 11:24:37.267	splunk web start				
2023-11-21 11:24:52.39	cat /etc/os-release				
2023-11-21 11:25:05.079	vim --version				
2023-11-21 11:25:31.208	sudo --version				
2023-11-21 11:26:03.34	ls --color=auto				
2023-11-21 12:23:58.888	cd /opt/splunk/bin/scripts/				
2023-11-21 12:24:00.158	cat shell.sh				
2023-11-21 12:24:28.888	id				



Containment

The attacker's attempt to upload "shell.xsl" to the system to exploit the "CVE-2023-46214" vulnerability on Splunk was detected in the proxy logs.

Afterwards, it was observed that the attacker received a reverse shell. Therefore, it is recommended to isolate the system from the network. The relevant operation can be done on Endpoint Security as follows.

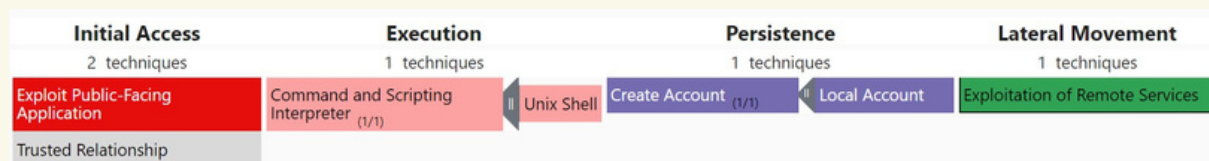


Lesson Learned

- Products should be kept up-to-date to avoid being affected by vulnerabilities.
- It is recommended not to open Splunk to Remote to avoid being affected by vulnerabilities.
- Access given to 3rd party companies should be restricted.
- Training should be provided periodically to increase information security awareness among users.
- Detection rules can be written in security products for IOCs reported with relevant vulnerabilities.

Appendix

MITRE



Artifacts

field	value
IPs	<ul style="list-style-type: none">• 180[.]101.88.240
files	<ul style="list-style-type: none">• shell.xsl• shell.sh
users	<ul style="list-style-type: none">• analysyt• admin
Host/IPs	<ul style="list-style-type: none">• Splunk Enterprise• 172.16.20.12• 3[.]133.116.124