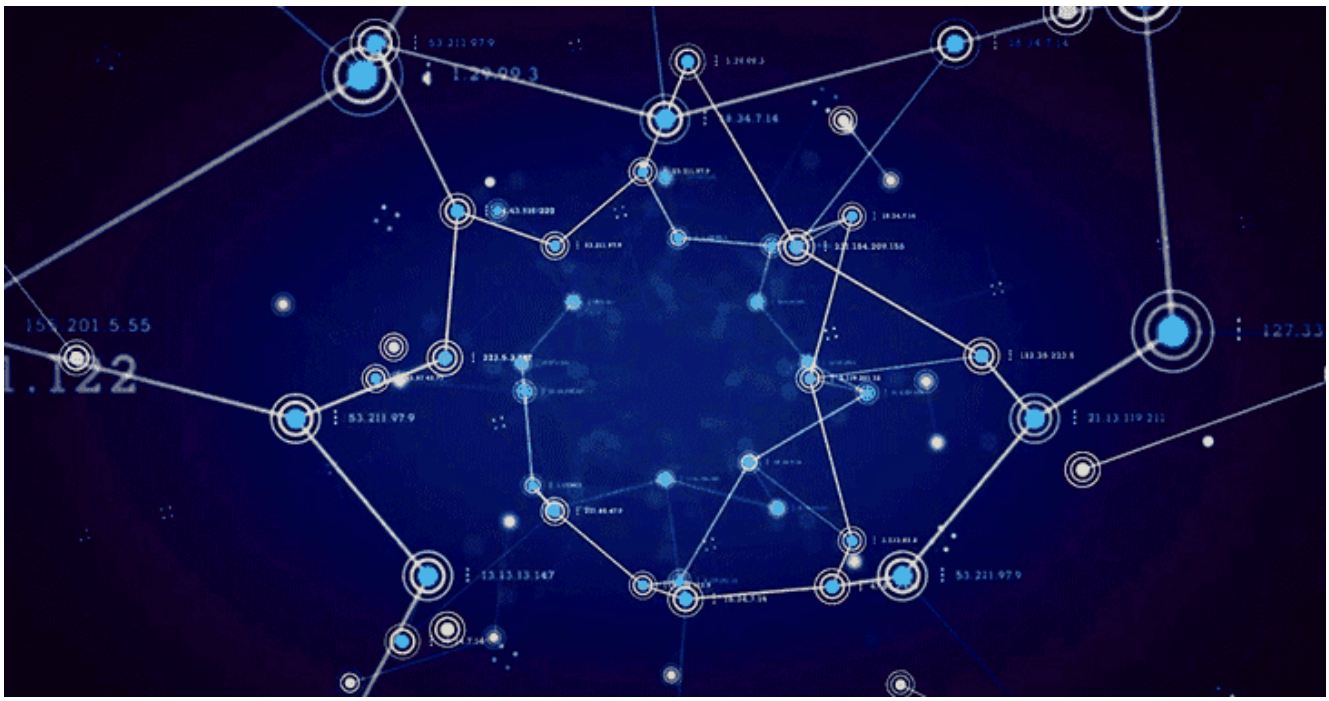
Hackers Exploiting Spring4Shell Vulnerability to Deploy Mirai Botnet Malware

thehackernews.com/2022/04/hackers-exploiting-spring4shell.html

April 8, 2022

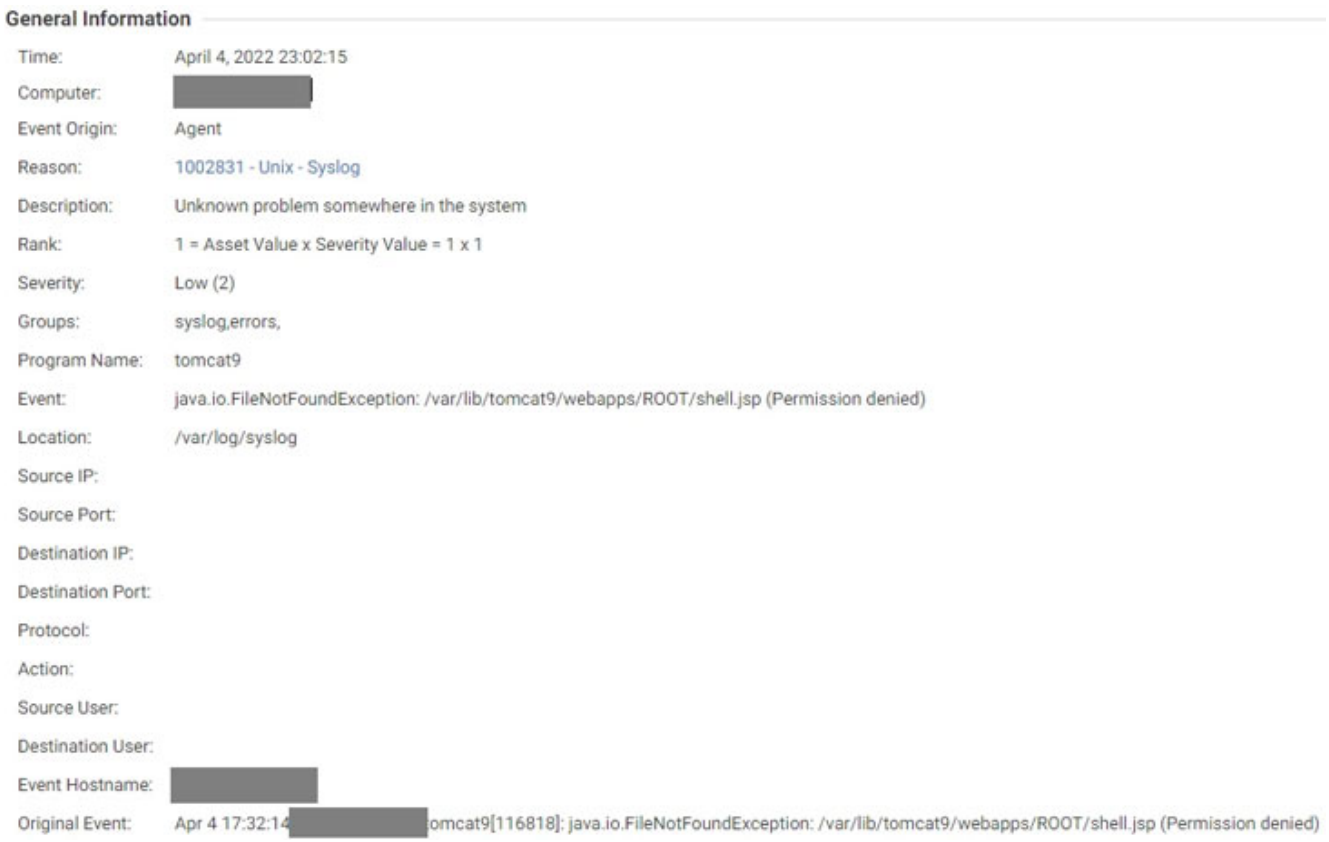


The recently disclosed critical **Spring4Shell** vulnerability is being actively exploited by threat actors to execute the Mirai botnet malware, particularly in the Singapore region since the start of April 2022.

"The exploitation allows threat actors to download the Mirai sample to the '/tmp' folder and execute them after permission change using 'chmod,'" Trend Micro researchers Deep Patel, Nitesh Surana, Ashish Verma said in a report published Friday.

Tracked as CVE-2022-22965 (CVSS score: 9.8), the vulnerability could allow malicious actors to achieve remote code execution in Spring Core applications under non-default circumstances, granting the attackers full control over the compromised devices.

The development comes as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) earlier this week added the Spring4Shell vulnerability to its Known Exploited Vulnerabilities Catalog based on "evidence of active exploitation."



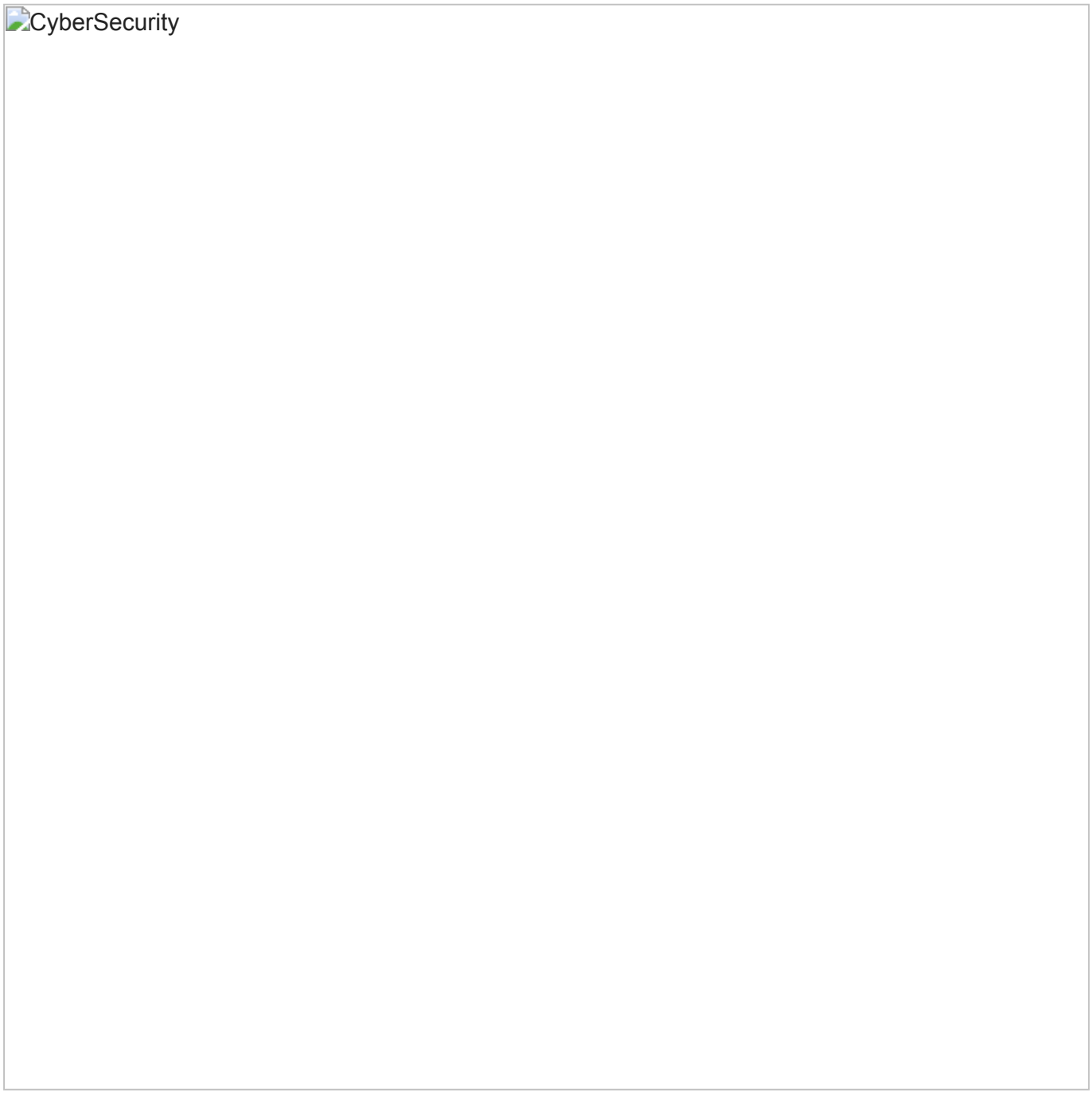
General Information

Time:	April 4, 2022 23:02:15
Computer:	[redacted]
Event Origin:	Agent
Reason:	1002831 - Unix - Syslog
Description:	Unknown problem somewhere in the system
Rank:	1 = Asset Value x Severity Value = 1 x 1
Severity:	Low (2)
Groups:	syslog,errors,
Program Name:	tomcat9
Event:	java.io.FileNotFoundException: /var/lib/tomcat9/webapps/ROOT/shell.jsp (Permission denied)
Location:	/var/log/syslog
Source IP:	
Source Port:	
Destination IP:	
Destination Port:	
Protocol:	
Action:	
Source User:	
Destination User:	
Event Hostname:	[redacted]
Original Event:	Apr 4 17:32:14 [redacted] tomcat9[116818]: java.io.FileNotFoundException: /var/lib/tomcat9/webapps/ROOT/shell.jsp (Permission denied)

This is far from the first time the botnet operators have quickly moved to add newly publicized flaws to their exploit toolset. In December 2021, multiple botnets including Mirai and Kinsing were uncovered leveraging the Log4Shell vulnerability to breach susceptible servers on the internet.

Mirai, meaning "future" in Japanese, is the name given to a Linux malware that has continued to target connected smart home devices such as IP cameras and routers and link them together into a network of infected devices known as a botnet.

The IoT botnet, using the herd of hijacked hardware, can be then used to commit further attacks, including large-scale phishing attacks, cryptocurrency mining, click fraud, and distributed denial-of-service (DDoS) attacks.



To make matters worse, the leak of Mirai's source code in October 2016 has given birth to numerous variants such as Okiru, Satori, Masuta, and Reaper, making it an ever-mutating threat.

"The [Mirai] code is so influential that even some of the malware offshoots are starting to have their own code versions released and co-opted by other cybercriminals," Intel 471 researchers said last month, pointing out the upload of the BotenaGo botnet's source code on GitHub in January 2022.

Earlier this January, cybersecurity firm CrowdStrike noted that malware hitting Linux systems increased by 35% in 2021 compared to 2020, with XOR DDoS, Mirai, and Mozi malware families accounting for more than 22% of Linux-targeted threats observed in the year.

"The primary purpose of these malware families is to compromise vulnerable internet-connected devices, amass them into botnets, and use them to perform distributed denial-of-service (DDoS) attacks," the researchers said.

SHARE □ □ □ □ □
SHARE □