RAVENii Report

SECURITY CONCERNS & EXPLOITS

July 6, 2020

Most of us spent the 4th of July holiday celebrating with family and friends and enjoying our extended weekends. Others spent the the 4th of July sleuthing around creating exploitable vulnerabilities for two commonly used technology tools: Palo Alto and F5 BIG IP Products.

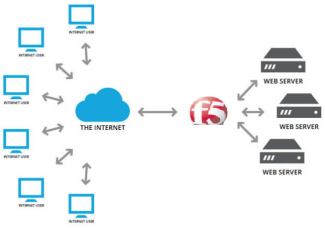
Palo Alto Networks

A major bug that lets hackers bypass authentication on the Palo Alto firewall and corporate VPN products has been discovered.

The US Cyber Command is urging consumers to make the necessary patches as soon as possible, especially if SAML is in use.

More information can be found here:
https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/us-cyber-command-says-foreign-hackers-will-attempt-to-exploit-new-pan-os-security-bug/

F5 BIG IP



A serious security issue that was disclosed by F5 before the holiday weekend is now being exploited in the wild.

The Traffic Management User Interface has a Remote Code Execution vulnerability. This vulnerability allows attackers to manipulate commands, files and services and could result in a complete system compromise.

More information can be found here:
https://support.f5.com/csp/article/K52145254?sf235665517=1

As always, RAVENii is here to help. Don't hesitate to reach out if you need us!