Public Comments for ICR 202207-1557-007

Author Full Name : Angel Grant **Received Date :** 09/06/2022 08:23 PM

Comments Received :

Please take the following recommendations on items to include in the update of the FFIEC Cybersecurity Assessment tool.

Domain 3- Cybersecurity Controls

- In accordance with warnings from the FBI and SEC, financial services organizations should take strong measures to prevent credential stuffing carried out by bots. Given the known sophistication of bots and the powerful motivation of criminals seeking to take over financial accounts, organizations should assume that bots will bypass defenses and therefore implement defenses that assume breach, which requires telemetry collection, machine learning to detect patterns of automation, and sophisticated code obfuscation to guard against reverse engineering and signal tampering.
- Preventative Controls/Infrastructure Management: Systems accessed from the Internet are monitoring and mitigating malicious automated requests/bots
- Detective Controls/Threat Vulnerability Detection: Anti-automation/bot tools are used to detect and mitigate attacks.
- Detective Controls/Anomalous Activity Detection: Controls are in place to detect anomalous activities from malicious automation/bots.
- To mitigate the risk of JavaScript supply chain attacks, attacks that result in formjacking, PII harvesting, and customer journey hijacking, financial services organizations should implement browser-based defenses that provide insights into the complete script behaviors and data exfiltration.

Domain 4 – External dependency management

- Add stronger focus on 3rd party risk assessments inclusive of open-sourced code & APIs
- Relationship Management/Ongoing Monitoring: Ongoing monitoring practice includes monitoring 3rd party applications for compromised or malicious application libraries.