CORTEX SYSTEMS INC. CYBERSECURITY INCIDENT REPORT FORM

State Agency: Cortex Systems Inc. Cybersecurity Division

Security Contact Information: security@cortexsystems.com | (555) 987-6543

Incident Reported By: Charles J. Wasson

Date of Report: March 28, 2025

Date & Time of Incident: March 28, 2025 | 2:14 PM EST

End Date & Time of Incident: March 28, 2025 | 2:55 PM EST

Summary of Incident

A SYN Flood Denial-of-Service (DoS) attack was detected targeting Cortex Systems Inc.'s public-facing web server. The web application became unresponsive after receiving an excessive number of TCP SYN requests from a suspicious IP address. The SYN packets initiated half-open TCP connections, overloading the server's connection queue and preventing legitimate user access. Wireshark confirmed the SYN flood pattern. The server was temporarily taken offline and the source IP was blocked. No evidence of data compromise or lateral movement was found.

What part of the system/network was affected?

- Public-facing web server (192.0.2.1)
- TCP Port 443 (HTTPS)
- Client access and internal usage were disrupted

What data or systems were impacted?

- No confirmed data loss or breach
- Temporary disruption to employee and customer access
- Service availability compromised (CIA Triad: Availability)

How was the incident detected?

Automated monitoring systems flagged unresponsive behavior on the web server. Wireshark analysis revealed an influx of SYN packets with no completed handshakes.

How was the incident contained?

The server was taken offline to clear connections. The attacker's IP address (203.0.113.0) was blocked at the firewall. Connection rates and SYN flood protection options are under review.

Description of Attachments

Wireshark TCP/HTTP log, internal response timeline, and cybersecurity incident report