**Post-Incident Report**

Date of investigation 11/18/2019

Date of incident 12/05/2018

Outcome - Intrusion through shellshock

Action Taken: Identified Attack vectors and host attempting attack, Advise closing off the attack points.

Reporting tool Snort

Attack vectors <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-7169> http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6278 http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6277 http://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271

Source IP | 172.18.0.3

Source port : A ton

Destination IP 172.18.0.2

Destination port 80

**Narrative**

• Alerted by Snort and Suricata:

◦ “OS-OTHER Bash CGI environment variable injection attempt

[Classification: Attempted Administrator Privilege Gain]”

• Located Source/Destination IP Addresses and timestamp from Alerts: Date/Time: 12/06-00:05:59.877941-12/06-00:05:59.948162

◦ Src/Prt: 72.18.0.3:47232/many more.

◦ Dst/Prt: 172.18.0.2:80

**Post-Incident Report**•

Identified Hostname and MacAddress of infected computer in pacp:

◦ MAC: 02:42:ac:12:00:03

Host Name: commix/v2.6-stable (http://commixproject.com)

**Post-Incident Report.**

• Identified tool used for attack: commix/v2.6-stable