FBI Cyber Division

Private Industry Notification

16 April 2014

PIN #: 140416 – 002

(U) UPDATE: Snort Signatures for Mitigation against Open Secure Socket Layer Heartbeat Extension Vulnerability

(U) This Private Industry Notification is an update to one previously released on 10 April 2014, and contains updated Snort rules for partner use.

(U) A serious vulnerability exists in the Open Secure Socket Layer (SSL) implementation of the Heartbeat extension. (1) CVE-2014-0160 exploitation may result in a leak of memory contents leading to the compromise of encryption keys, authentication keys, user credentials or other data from Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) clients and servers.

(U) The affected versions of OpenSSL software are versions 1.0.1 through 1.0.1f. Versions prior to 1.0.1 are unaffected and versions 1.0.1g and later have implemented a fix for the vulnerability.

(U) The following Snort signatures have been developed and tested to detect attempted exploitation of the vulnerability by know open source exploitation techniques. They are bi-directional to detect client-to-server and server-to-client requests. It is recommended that these signatures be immediately implemented at lower levels as well.

(U) Snort Signatures:

alert tcp $EXTERNAL_NET any -> $HOME_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL SSLv3 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03 00|"; depth:3; detection_filter:track by_src, count 3, seconds 1; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30510; rev:5;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03 01|"; depth:3; detection_filter:track by_src, count 3, seconds 1; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30511; rev:5;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03 02|"; depth:3; detection_filter:track by_src, count 3, seconds 1; metadata:policy balanced-

ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30512; rev:5;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03 03|"; depth:3; detection_filter:track by_src, count 3, seconds 1; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30513; rev:5;)

alert tcp $HOME_NET [25,443,465,636,992,993,995,2484] -> $EXTERNAL_NET any (msg:"SERVER-OTHER SSLv3 large heartbeat response - possible ssl heartbleed attempt"; flow:to_client,established; content:"|18 03 00|"; depth:3; byte_test:2,>,128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30514; rev:6;)

alert tcp $HOME_NET [25,443,465,636,992,993,995,2484] -> $EXTERNAL_NET any (msg:"SERVER-OTHER TLSv1 large heartbeat response - possible ssl heartbleed attempt"; flow:to_client,established; content:"|18 03 01|"; depth:3; byte_test:2,>,128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30515; rev:6;)

alert tcp $HOME_NET [25,443,465,636,992,993,995,2484] -> $EXTERNAL_NET any (msg:"SERVER-OTHER TLSv1.1 large heartbeat response - possible ssl heartbleed attempt"; flow:to_client,established; content:"|18 03 02|"; depth:3; byte_test:2,>,128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30516; rev:6;)

alert tcp $HOME_NET [25,443,465,636,992,993,995,2484] -> $EXTERNAL_NET any (msg:"SERVER-OTHER TLSv1.2 large heartbeat response - possible ssl heartbleed attempt"; flow:to_client,established; content:"|18 03 03|"; depth:3; byte_test:2,>,128,0,relative; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30517; rev:6;)

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL SSLv3 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03 00|"; depth:3; byte_test:2,>,128,3; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-admin; sid:30520; rev:3;)

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03 01|"; depth:3; byte_test:2,>,128,3; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-admin; sid:30521; rev:3;)

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03

02|"; depth:3; byte_test:2,>,128,3; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-admin; sid:30522; rev:3;)

alert tcp $HOME_NET any -> $EXTERNAL_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt"; flow:to_server,established; content:"|18 03 03|"; depth:3; byte_test:2,>,128,3; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-admin; sid:30523; rev:3;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt"; flow:to_server,established; dsize:8; content:"|18 03 02 00 03 01 40 00|"; depth:8; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30524; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET [25,443,465,636,992,993,995,2484] (msg:"SERVER-OTHER OpenSSL TLSv1.2 heartbeat read overrun attempt"; flow:to_server,established; dsize:69; content:"|18 03 03 00 40|"; depth:5; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service ssl; reference:cve,2014-0160; classtype:attempted-recon; sid:30525; rev:1;)

(U) Reporting Notice

(U) The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI Cyber Task Force or Cyber Watch (CyWatch), by telephone at 855-292-3937 or by e-mail at cywatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Administrative Notes: Law Enforcement Response

(U) Information contained in this product is UNCLASSIFIED. There is no additional information available on this topic.

(U) For comments or questions related to the content or dissemination of this document, please reference CYD-CC-1677.