TLP: WHITE
MS-ISAC CYBER ALERT

TO: All MS-ISAC Members, Fusion Centers, and Intel Partners

DATE: August 28, 2017

SUBJECT: MS-ISAC CYBER ALERT – DNSSEC Key Signing Key Rollover

The Internet Corporation for Assigned Names and Numbers (ICANN) announced that on October 11, 2017, it will be changing the Root Zone Key Signing Key (KSK) used in the Domain Name System (DNS) Security Extensions (DNSSEC) protocol. DNSSEC is a set of opt-in protocols that digitally sign DNS information, providing source authentication and integrity protection. The DNS Root Zone (".") is the top node of the DNS tree and clients configured to use the DNS Root Zone key are able to validate any DNSSEC signed zone.

Changing keys, a.k.a. key rollover, is necessary to maintain a secure protocol. This rollover only affects DNS recursive resolvers that are configured to use DNSSEC. If DNSSEC is not configured in your environment, no changes are required. If DNSSEC is configured, then maintaining an up-to-date Root Zone KSK is essential to ensuring DNS resolvers continue to function after the rollover. To do this you have two options: configure automated key rollover or update the key manually.

Important Dates:

- **September 19, 2017:** Size increase for DNSKEY response from root name servers.
- **October 11, 2017:** New KSK begins to sign the root zone key set.
- **January 11, 2018:** Revocation of old KSK.
- **March 22, 2018:** Last day the old KSK appears in the root zone.
- **August 2018:** Old key is deleted from equipment in both ICANN Key Management Facilities.

A test platform to ensure systems are ready is available at: https://automated-ksk-test.research.icann.org/. Per ICANN, the test validates support for RFC 5011 automated trust anchor update protocol and therefore a systems readiness for the root zone KSK roll. System administrators should be aware that the ICANN states that the test takes about 45 days, but the most important results are available about 30 days after the test begins.

RECOMMENDATIONS:
MS-ISAC recommends organizations inventory their DNS servers to determine if DNSSEC is currently securing their DNS architecture and if so, plan to ensure keys are rolled over through an automated key rollover or a manual update.

REFERENCES:
https://www.icann.org/resources/pages/ksk-rollover
https://rollready.dnsops.gov/
https://www.us-cert.gov/ncas/current-activity/2017/08/21/DNSSEC-Key-Signing-Key-Rollover-0
https://www.nanog.org/sites/default/files/20170203_Lewis_2017_Dnssec_Ksk_v1.pdf

DNS Test information
https://automated-ksk-test.research.icann.org/

DNSSEC information
http://dnssec.net/

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/