Dear Registrar,

In early January 2020, it was announced that researchers had computed the very first chosen-prefix collision for the SHA-1 hash algorithm. In general terms, this first practical implementation of the attack has the potential for dangerous and far-reaching consequences in the Domain Name System (DNS) ecosystem, including use against Domain Name System Security Extensions (DNSSEC).

What is SHA-1?
SHA-1 is a cryptographic hash algorithm that has been widely used in a variety of security applications and protocols to authenticate data. Hash algorithms are used to create short strings of bits, known as hash values, that can represent longer messages similar to a fingerprint. One of the properties of strong hash algorithms is that it makes it extremely difficult to create two different messages that have the same hash value. Like most security protocols on the Internet, DNSSEC uses hash algorithms to increase the speed of signing and validating signatures.

Who is Affected and How?
The attacks on SHA-1 can affect anyone who directly or indirectly manages a signed DNS zone, including registries, registrars, registrants, and anyone offering DNS hosting services.

Recommended Action
The ICANN organization, along with the cryptographic community, highly recommend migrating away from the use of SHA-1 in DNSSEC zone signatures and to instead use algorithms 8 (RSA with SHA-256) or 13 (ECDSA Curve P-256 with SHA-256). Although the use of SHA-1 in DS records does not appear to be immediately at risk by this attack, the cryptographic community already recommends using either SHA-256 or SHA-384. (Note that use of SHA-1 in NSEC3 does not appear to be vulnerable to this new attack.)

If you have a provider managing your DNS zones on your behalf, please contact them to assess whether or not you may be impacted. If you are using SHA-1 for signing your DNS zone, definitely consider migrating to stronger algorithms outlined above. Review the DNSSEC Operational Practices described inRFC 6781, particularly those related to algorithm rollovers in Section 4.1.4, and the Key Rollover Timing Considerations described in RFC 7583.

As described in the DNSSEC paper, parties accepting DNS records or other third party data that will be signed into their DNS zones are most at risk. It may be beneficial for such parties to immediately consider the handling of this type of data to ensure it is properly validated to reduce the potential of abuse. Additional protections like not sharing signing keys and having separate ZSKs and KSKs should be taken into account.

Due to the nature of the attack and the heightened awareness surrounding it, anyone still using SHA-1 in DNSSEC should implement these changes as soon as practically possible. Although

not an emergency, getting ahead of this vulnerability will not only ensure system security but avoid last minute emergencies as it's expected for the attacks to get better with time.

More Information
ICANN org has published a blog on the issue and its implications, available here. If you have any questions on this issue, please feel free to reach out to ICANN org's Global Support Center.

Regards,

Technical Services Team
Global Domains Division
Internet Corporation for Assigned Names and Numbers (ICANN)