REGEXT Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 14 September 2025

S. Hollenbeck
Verisign Labs
W. Carroll
Verisign
G. Akiwate
Stanford University

13 March 2025

Best Practices for Deletion of Domain and Host Objects in the Extensible Provisioning Protocol (EPP)
draft-ietf-regext-epp-delete-bcp-10

Abstract

The Extensible Provisioning Protocol (EPP) includes commands for clients to delete domain and host objects, both of which are used to publish information in the Domain Name System (DNS). EPP also includes guidance for deletions that is intended to avoid DNS resolution disruptions and maintain data consistency. However, operational relationships between objects can make that guidance difficult to implement. Some EPP clients have developed operational practices to delete those objects that have unintended impacts on DNS resolution and security. This document describes best current practices and proposes new potential practices to delete domain and host objects that reduce the risk of DNS resolution failure and maintain client-server data consistency.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 14 September 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Section 3.2.2 of RFC 5731 [RFC5731] contains text that has led some domain name registrars (acting as EPP clients) to adopt an operational practice of re-naming name server host objects so that they can delete domain objects:

"A domain object SHOULD NOT be deleted if subordinate host objects are associated with the domain object. For example, if domain "example.com" exists and host object "ns1.example.com" also exists, then domain "example.com" SHOULD NOT be deleted until host "ns1.example.com" has either been deleted or renamed to exist in a different superordinate domain."

Similarly, Section 3.2.2 of RFC 5732 [RFC5732] contains this text regarding deletion of host objects:

"A host name object SHOULD NOT be deleted if the host object is associated with any other object. For example, if the host object is associated with a domain object, the host object SHOULD NOT be deleted until the existing association has been broken. Deleting a host object without first breaking existing associations can cause DNS resolution failure for domain objects that refer to the deleted host object."

These recommendations create a dilemma when the sponsoring client for "example.com" intends to delete "example.com" but its associated host object "ns1.example.com" is also associated with domain objects sponsored by another client. It is advised not to delete the host object due to its associated domain objects. However, the associated domain objects cannot be directly updated because they are sponsored by another client. This situation affects all EPP operators that have implemented support for host objects.

Section 3.2.5 of RFC 5732 [RFC5732] describes host object renaming:

"Host name changes can have an impact on associated objects that refer to the host object. A host name change SHOULD NOT require additional updates of associated objects to preserve existing associations, with one exception: changing an external host object that has associations with objects that are sponsored by a different client. Attempts to update such hosts directly MUST fail with EPP error code 2305. The change can be provisioned by creating a new external host with a new name and any needed new attributes, and subsequently updating the other objects sponsored by the client."

Section 1.1 of RFC 5732 includes a description of external hosts. Some EPP clients have developed operational practices that use host object renaming to break association between a domain object and host object. Note that the specific method used to rename the host object can create DNS delegation failures and introduce risks of loss of management control. If the new external host refers to an unregistered domain, then a malicious actor may register the domain and create the host object to gain control of DNS resolution for the domain previously associated with "ns1.example.com". If the new

external host offers an authoritative DNS service but the domain is not assigned to an account, then a malicious actor may add the domain to a service account and gain control of (hijack) DNS resolution functionality. If the new external host offers recursive DNS service or no DNS service, then DNS requests for the domain will result in SERVFAIL messages or other errors. Aggressive re-queries by DNS resolvers may then create large numbers of spurious DNS queries for an unresolvable domain. Note that renaming a host object to a name of an external host cannot be reversed by the EPP client.

This document describes the rationale for the "SHOULD NOT be deleted" text and the risk associated with host object renaming. Section 5 includes a detailed analysis of the practices that have been and can be used to mitigate that risk. Section 6 includes specific recommendations for the best practices.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Rationale for "SHOULD NOT be deleted"

3.1. DNS Considerations

The primary consideration when deleting domain and host objects concerns the potential impact on DNS resolution. Deletion of a domain object will make all name servers associated with subordinate host objects unresolvable. Deletion of a host object will make any domain that has been delegated to the associated name server unresolvable. The text in RFCs 5731 and 5732 was written to encourage clients to take singular, discrete steps to delete objects in a way that avoids breaking DNS resolution functionality. Additionally, allowing host objects to exist after deletion of their superordinate domain object invites hijacking, as a malicious actor may re-register the domain object, potentially controlling resolution for the host objects and for their associated domain objects. It also creates orphan glue as described in SAC048 ([SAC048]).

3.2. Client-Server Consistency Considerations

A server that implicitly deletes subordinate host objects in response to a request to delete a domain object can create a data inconsistency condition in which the EPP client and the EPP server have different views of what remains registered after processing a <delete> command. The text in RFCs 5731 and 5732 was written to encourage clients to take singular, discrete steps to delete objects in a way that maintains client-server data consistency. Experience suggests that this inconsistency poses little operational risk.

3.3. Relational Consistency Considerations

Implementations of EPP can have dependencies on the hierarchical domain object/host object relationship, as can exist in a relational database. In such instances, deletion of a domain object without addressing the existing subordinate host objects can cause relational consistency and integrity issues. The text in RFCs 5731 and 5732 was written to reduce the risk of these issues arising as a result of implicit object deletion.

4. Host Object Renaming Risk

As described in RFC 5731, it is possible to delete a domain object that has associated host objects that are managed by other clients by renaming the host object to exist in a different superordinate domain. This is commonly required when the sponsoring client is unable to disassociate a host object from a domain object managed by another client because only the second client is authorized to make changes to their domain object and the EPP server requires host object disassociation to process a request to delete a domain object. For example:

Domain object "domain1.example" is registered by ClientX.

Domain object "domain2.example" is registered by ClientY.

Subordinate host object "ns1.domain1.example" is registered and associated with domain object "domain1.example" by ClientX.

Host object "ns1.domain1.example" is associated with domain object "domain2.example" by ClientY.

ClientX wishes to delete domain object "domain1.example". It can modify domain object "domain1.example" to remove the association of host object "ns1.domain1.example", but ClientX cannot remove the association of host object "ns1.domain1.example" from domain object "domain2.example" because "domain2.example" is sponsored by ClientY

and ClientX is unable to determine that relationship. Only ClientY can modify domain object "domain2.example", and if they do not do so ClientX will need to rename host object "ns1.domain1.example" so that "domain1.example" can be deleted.

ClientX renames host object "ns1.domain1.example" to "ns1.example.org", creating an external host and meeting the EPP server's subordinate host object disassociation requirement. The renamed host object "ns1.example.org" is referred to as a "sacrificial" host [risky-bizness].

If domain "example.org" does not exist, this practice introduces a risk of DNS resolution hijacking if someone were to register the "example.org" domain and create a subordinate host object named "ns1.example.org". That name server would receive DNS queries for all domains delegated to it, allowing the operator of the name server to respond in potentially malicious ways.

5. Analysis of Practices for Domain and Host Object Deletion

EPP servers can employ a range of practices for domain and host object deletion. Notably, the scope of any practice discussed here is the EPP server that adopts the practice and the domains managed by it. The practices described in this document fall into two broad categories: renaming objects to use "sacrificial" hosts, and allowing objects to be deleted even if there are existing data relationships. These practice categories are described in the following sections. For a broader consideration of practices and potential impacts on registries and registrars, [SAC125] offers some complementary insight.

5.1. Renaming to Sacrificial Hosts

"Sacrificial" hosts are hosts whose name is intended to remove an existing relationship between domain and host objects. To that end, "sacrificial" hosts are either renamed to an external host or associated with a different domain object in the EPP server. The first group of deletion practices use sacrificial hosts leveraging existing EPP server support for renaming host objects.

5.1.1. Practice Benefits

Affected domains remain delegated in the zone. Registrars and registrants of affected domains may be able to determine the intention of the change.

5.1.2. Practice Detriments

Zones are crowded with irrelevant records. Registrars and registrants of affected domains are required to clean them up.

5.1.3. Observed Practices for Renaming to Sacrificial Hosts

5.1.3.1. Renaming to External, Presumed Non-Existent Hosts

As described above, this practice renames subordinate host objects to an external host in order to allow the deletion of the superordinate domain object. The external host is presumed to be non-existent by the deleting EPP client but no check for existence is typically performed. This practice has been observed in use. This practice MUST NOT be used.

5.1.3.1.1. Practice Benefits

The primary benefit is convenience for the deleting EPP client. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic.

5.1.3.1.2. Practice Detriments

Malicious actors have registered these parent domains and created child host objects to take control of DNS resolution for associated domains [risky-bizness].

Sponsoring clients of the associated domains are not informed of the change. Associated domains may no longer resolve if all their hosts are renamed. Associated domains may still resolve if they continue to be associated with existent hosts, in which case their partial vulnerability to hijacking is more difficult to detect.

5.1.3.2. Renaming to "as112.arpa"

Some domain registrars, acting as EPP clients, have renamed host objects to subdomains of "as112.arpa" or "empty.as112.arpa" [risky-bizness-irtf]. This practice has been observed in use.

5.1.3.2.1. Practice Benefits

The primary benefit is convenience for the deleting EPP client. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic.

5.1.3.2.2. Practice Detriments

This is a misuse of AS112, which is for reverse lookups on non-unique IPs, primarily so local admins can sinkhole non-global traffic [RFC7535]. The "empty.as112.arpa" is designed to be used with DNAME aliasing, not as a parent domain for sacrificial name servers (see section 3 of [RFC7535]). Unexpected AS112 traffic has previously caused problems with intrusion detection systems and firewalls [RFC6305]. Local administrators can potentially hijack requests. AS112 infrastructure must be maintained.

5.1.3.3. Renaming to Non-Authoritative Hosts

Some domain registrars, acting as EPP clients, have maintained host objects with glue records pointing to prominent public recursive DNS services. This practice has been observed in use. This practice MUST NOT be used.

5.1.3.3.1. Practice Benefits

The primary benefit is convenience for the deleting EPP client. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic.

5.1.3.3.2. Practice Detriments

Queries for the associated domains result in SERVFAIL or other failure responses. Some recursive name server implementations may aggressively re-query for these responses, potentially resulting in large numbers of queries for unresolvable domains [RFC9520].

5.1.3.4. Renaming to Client-Maintained Dedicated Sacrificial Name Server Host Objects

EPP clients MAY rename the host object to be deleted to a sacrificial name server host object maintained by the client. This requires that the client maintain the registration of the sacrificial name server's superordinate domain. The client may consider long registration periods and the use of registrar and registry lock services to maintain and protect the superordinate domain and the host object. Failures to maintain these registrations have allowed domain hijacks [risky-bizness].

The client-maintained dedicated sacrificial name server MUST resolve to one or more IP addresses and the client MUST operate an authoritative DNS name server on those addresses. The name server MAY provide any valid response.

This practice has been observed in use.

5.1.3.4.1. Practice Benefits

Associated domains are not able to be hijacked, remain in the zone, and have valid DNS records and a responsive DNS service. The service may provide responses that indicate problems with a domain's delegation, such as non-existence or include controlled interruption IP addresses [RFC8023].

5.1.3.4.2. Practice Detriments

This requires that the client maintain the registration of the sacrificial name server's superordinate domain. The client may consider long registration periods and the use of registrar and registry lock services to maintain and protect the superordinate domain and the host object. Failures to maintain these registrations have allowed domain hijacks [risky-bizness].

Failure responses may cause aggressive requerying (see Section 5.1.3.3.2).

5.1.4. Potential Practices for Renaming to Sacrificial Hosts

5.1.4.1. Renaming to Pseudo-TLD

Clients may rename host objects to use ".alt" or another non-DNS pseudo-TLD as suggested in [risky-bizness-irtf]. This practice has not been observed in use. This practice MUST NOT be used.

5.1.4.1.1. Practice Benefits

The primary benefit is convenience for the deleting EPP client. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic. Dependent domains cannot be hijacked through the registration of these identifiers and delegation in the DNS.

5.1.4.1.2. Practice Detriments

The ".alt" pseudo-TLD is to be used "to signify that this is an alternative (non-DNS) namespace and should not be looked up in a DNS context" [RFC9476]. Some EPP servers may restrict TLDs to valid IANA-delegated TLDs. These entries would mix DNS and non-DNS protocols, risk name collisions, create confusion, and potentially result in unpredictable resolver behaviors. These identifiers may be registered in non-DNS namespaces, potentially leading to hijacking vulnerabilities based in other systems.

5.1.4.2. Renaming to Existing Special-Use TLD

Clients may rename host objects to a special-use TLD that cannot resolve in the DNS. Several variations have been suggested. This practice has not been observed in use.

5.1.4.2.1. Renaming to Reserved TLD

Clients may rename host objects to use a reserved special-use ([RFC6761]) TLD as suggested in [risky-bizness].

5.1.4.2.1.1. Practice Benefits

The primary benefit is convenience for the deleting EPP client. These TLDs are already reserved and will not resolve. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic. Dependent domains cannot be hijacked.

5.1.4.2.1.2. Practice Detriments

The use of TLDs reserved for special purposes ([RFC6761]) may be confusing without a domain designated by the community for this purpose (see "sacrificial.invalid" in Section 5.1.4.3 and Section 6). In addition, their use may be prevented by EPP server policy.

5.1.4.3. Renaming to a Special-Use Domain

Clients would rename hosts to a special-use domain or subdomain thereof. The domain may be a special-use SLD (e.g., sacrificial.invalid) or a new reserved TLD (e.g., .sacrificial). Use of this domain would communicate the client’s intention to create a sacrificial host. IANA would add this domain to the "Special-Use Domain Name" registry if such a new TLD is created using either IETF or ICANN processes. This practice has not been observed in use. In terms of the questions from [RFC6761]:

1. These names are not expected to be visible to human users. However, the purpose of these domains is expected to be semantically recognizable to human users.

2. Application software is not expected to recognize these names as special or treat them differently than other allowed domain names.

3. Name resolution APIs and libraries are not expected to recognize these names as special or treat them differently than other allowed domain names.

4. Caching name servers are not expected to recognize these names as special or treat them differently than other allowed domain names.

5. Authoritative name servers are not expected to recognize these names as special or treat them differently than other allowed domain names. Requests to the root for this domain would result in NXDOMAIN response [RFC8499].

6. DNS server operators will treat this domain and its subdomains as they would any other allowed names in the DNS.

7. DNS Registries/Registrars will not be able to register this domain and must deny requests to register it or its subdomains.

5.1.4.3.1. Practice Benefits

This option would offer clarity concerning the intentions of registrars that rename hosts. It would also enable registrars of affected domains ease of detection of renamed hosts. This option is also convenient for the deleting EPP client. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic. Dependent domains cannot be hijacked through the registration of these identifiers and delegation in the DNS.

5.1.4.3.2. Practice Detriments

This would require cooperation and policy changes for registrars and registries.

5.1.4.4. Renaming to Community Sacrificial Name Server Service

A new community-wide service could be created explicitly intended for use for renaming host records. This would require maintenance of name servers capable of authoritatively responding with NXDOMAIN or a controlled interruption IP addresses [RFC8023] for all queries without delegating domains or records. This service could use a new special-use TLD created either through ICANN or IETF processes (e.g., ".sacrificial"), as an IAB request that IANA delegate a second-level domain (SLD) for ".arpa" (e.g., "sacrificial-nameserver.arpa"), or as a contracted sinkhole service by ICANN or other DNS ecosystem actors. This practice has not been observed in use.

5.1.4.4.1. Practice Benefits

This is convenient for the deleting EPP client. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic. The associated domains are not vulnerable to hijacking. This would provide a well-understood, industry-standard solution, allowing registrars and registrants to easily identify associated domains that have been affected. Infrastructure operators could monitor traffic to identify affected associated domains that result in significant traffic and attempt to contact registrars and registrants. Economies of scale would allow reduced overall costs to the industry (in contrast to each client running an independent service).

5.1.4.4.2. Practice Detriments

Some entity must maintain the infrastructure for the service.

5.2. Deletion of Hosts

The second group of practices is based on EPP server support for allowing objects to be deleted even if there are existing data relationships. The recommendations in RFC 5731 [RFC5731] are intended to maintain consistency. However, they are not requirements.

5.2.1. Observed Practices for Deletion of Hosts

5.2.1.1. Implicit Delete of Affected Host Objects

EPP servers may relax their constraints and allow sponsoring clients to delete host objects without consideration of associations with domain objects sponsored by other clients. The registry automatically disassociates the deleted host objects from domain objects sponsored by other clients. This practice has been observed in use.

5.2.1.1.1. Practice Benefits

This is convenient for the deleting EPP client. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic. The associated domains are not vulnerable to hijacking.

5.2.1.1.2. Practice Detriments

This could result in domains with no remaining name servers being removed from the zone or domains with only one remaining name server. Deletions could potentially affect large numbers of associated domains, placing strain on domain registries.

5.2.1.2. Inform Affected Clients

The sponsoring clients of affected domain objects may also be informed of the change (e.g., through the EPP Change Poll extension [RFC8590]). This practice has been observed in use.

5.2.1.2.1. Practice Benefits

Updates help achieve the goals of client-server data consistency and minimal interruptions to resolution. The sponsoring clients of affected domain objects are able to update their database to reflect the change and would be able to inform the domain’s registrant. The sponsoring clients can automatically update the affected domains to use another authoritative host.

5.2.1.2.2. Practice Detriments

This change requires additional development on the part of EPP servers and clients. There may be scalability concerns if large numbers of domain objects are updated in a single transaction.

5.2.2. Potential Practices for Deletion of Hosts

5.2.2.1. Request Explicit Delete of Affected Host Objects

Sponsoring clients requesting the deletion of host objects would explicitly request their disassociation from domain objects sponsored by other clients. This practice has not been observed in use.

5.2.2.1.1. Practice Benefits

Registries would not be required to unilaterally take responsibility for deletion. The deleting EPP client is not required to maintain an authoritative DNS service or receive traffic. The associated domains are not vulnerable to hijacking.

5.2.2.1.2. Practice Detriments

This could result in domains with no remaining name servers being removed from the zone or domains with only one remaining name server. Deletions could potentially affect large numbers of associated domains, placing strain on domain registries.

5.2.2.2. Provide Additional Deletion Details

The EPP server may provide the deleting EPP client with additional details of the affected objects. The deleting EPP client may receive a response (e.g., using msg, reason, msgQ elements of the EPP response [RFC5730]) that deletion of the host object would affect domain objects sponsored by another client and may receive details about those objects (e.g., using the EPP poll command). This practice has not been observed in use.

5.2.2.2.1. Practice Benefits

The deleting EPP client would be able to better understand and assess the potential harms of host object deletion. Depending on the content of the message, the deleting EPP client might choose additional actions, such as delaying the deletion until manual approval can be obtained, renaming the host objects, or informing affected EPP clients. This would give EPP clients greater flexibility with respect to deletion. For example, they may choose only to exercise deletions that have no impact on other clients.

5.2.2.2.2. Practice Detriments

This change would require additional development on the part of EPP servers and clients. There may be scalability concerns if large numbers of domain objects are updated in a single transaction. The EPP server must determine the relevant information to provide for the EPP client’s assessment.

5.2.2.3. Allow Explicit Delete of Domain with Restore Capability

Explicit deletion of a domain name with a cascade purge of subordinate host objects and associations with other domains may be an unrecoverable operation, increasing the potential negative effects of malicious or accidental actions.

To mitigate this risk, EPP servers can allow for the explicit deletion of a domain with subordinate host objects associated with other domains only when the associations can be restored by the <restore> operation described in RFC 3915 [RFC3915].

In order to allow restore, EPP servers may keep the subordinate host objects with a "pendingDelete" status and keep associations with other domains. This makes the objects unavailable in the DNS and provides a preview of the deletion.

If the action was malicious, accidental, or had negative side effects, the domain, its subordinate host objects, and the associations with other domains can be restored with the <restore> operation in RFC 3915 during the redemption period. The purge of the domain will correspond with the purging of the subordinate hosts objects and the associations at the end of the pending delete period in RFC 3915.

Due to the potentially large number of associations, the server can asynchronously update (e.g., add and remove from DNS) and purge the associations.

This practice has not been observed in use.

5.2.2.3.1. Practice Benefits

This practice enables the clients to directly delete the domains that they need since the server will fully support restoration of the associations during the redemption period. The management of the domain and the subordinate hosts will be simplified for the client by supporting the explicit deletion of the domain with the capability of mitigating a destructive malicious or accidental action.

5.2.2.3.2. Practice Detriments

By making it easier for a client to explicitly delete a domain having subordinate hosts with associations, there is higher risk of inadvertent side effects in a single delete command. There is existing risk in EPP of inadvertent side effects, such as adding the "clientHold" status to the domain that will impact the DNS resolution of the subordinate hosts and the associated delegations. The ability to easily rollback the command is key to minimize the impact of the side effects. Another issue is the potential size of the database transaction to disable, re-enable, or purge the subordinate host associations, since there is no limit to the number of associations to delegated domains. Servers can break-up the disable, re-enable, or purge of the subordinate host associations into smaller transactions by implementing it asynchronously.

6. Recommendations

EPP servers and clients MUST implement one of the following practices to delete domain and host objects with minimal undesired side effects:

* Rename host objects to a sacrificial name server host object maintained by the client (see 5.1.3.4).

* Delete host objects and associations with the restore option (see 5.2.2.3) based on explicit client requests (see 5.2.2.1). Provide requesting clients additional deletion details (see 5.2.2.2) and inform affected clients of changes (see 5.2.1.2).

* Rename host objects to a sacrificial name server host object that uses a special-use domain (see 5.1.4.3) that avoids the special-use domain issues described in [RFC8244]. Use of "sacrificial.invalid" (see 5.1.4.3) as the parent domain for the host objects is RECOMMENDED to avoid the overhead of creating a new TLD using either IETF or ICANN processes that offers no additional operational benefit.

All other practices described in Section 5 are NOT RECOMMENDED due to undesired side effects.

7. IANA Considerations

This document does not contain any instructions for IANA.

8. Security Considerations

This document describes guidance found in RFCs 5731 and 5732 regarding the deletion of domain and host objects by EPP clients. That guidance sometimes requires that host objects be renamed such that they become "external" hosts (see Section 1.1 of RFC 5731 [RFC5731]) in order to meet an EPP server’s requirements for host object disassociation prior to domain object deletion. Host object renaming can introduce a risk of DNS resolution hijack under certain operational conditions. This document provides guidance that is intended to reduce the risk of DNS resolution failure or hijacking as part of the process of deleting EPP domain or host objects.

Child domains that depend on host objects associated with domain objects sponsored by another EPP client for DNS resolution may be protected from hijacking through the use of DNSSEC. Their resolution may be protected from the effects of deletion by using host objects associated with multiple domain objects. DNSSEC and multiple host objects may interfere with the use of controlled interruption IP

addresses to alert registrants to DNS changes. EPP clients can periodically scan sponsored domains for association with sacrificial name servers and alert end users concerning those domains.

In absence of DNSSEC use by the victim, an attacker who gains control of a single nameserver can use DNSSEC to instead take over the victim domain completely if the registry operator and registrar process for automated DS maintenance neglects to check all nameservers for consistency in CDS/CDNSKEY records. In this scenario, the domain will end up with DS records derived from the attacker CDS/CDNSKEY records if, by chance, the queries happen to hit the attacker controlled nameserver. Subsequently, validating resolvers will no longer accept responses from the legitimate nameservers. Moreover, with the use of CSYNC an attacker may update the domain NS records removing the legitimate nameservers entirely.

9. Acknowledgments

The authors would like to thank the following people for their contributions to this document: Brian Dickson, James Gould, Pawel Kowalik, Mario Loffredo, James Mitchell, Matthew Thomas, Peter Thomassen, Duane Wessels, David Blacka.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3915] Hollenbeck, S., "Domain Registry Grace Period Mapping for the Extensible Provisioning Protocol (EPP)", RFC 3915, DOI 10.17487/RFC3915, September 2004, <https://www.rfc-editor.org/info/rfc3915>.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009, <https://www.rfc-editor.org/info/rfc5730>.

[RFC5731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", STD 69, RFC 5731, DOI 10.17487/RFC5731, August 2009, <https://www.rfc-editor.org/info/rfc5731>.

[RFC5732] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Host Mapping", STD 69, RFC 5732, DOI 10.17487/RFC5732, August 2009, <https://www.rfc-editor.org/info/rfc5732>.

[RFC6761] Cheshire, S. and M. Krochmal, "Special-Use Domain Names", RFC 6761, DOI 10.17487/RFC6761, February 2013, <https://www.rfc-editor.org/info/rfc6761>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8244] Lemon, T., Droms, R., and W. Kumari, "Special-Use Domain Names Problem Statement", RFC 8244, DOI 10.17487/RFC8244, October 2017, <https://www.rfc-editor.org/info/rfc8244>.

[RFC9476] Kumari, W. and P. Hoffman, "The .alt Special-Use Top-Level Domain", RFC 9476, DOI 10.17487/RFC9476, September 2023, <https://www.rfc-editor.org/info/rfc9476>.

10.2. Informative References

[RFC6305] Abley, J. and W. Maton, "I’m Being Attacked by PRISONER.IANA.ORG!", RFC 6305, DOI 10.17487/RFC6305, July 2011, <https://www.rfc-editor.org/info/rfc6305>.

[RFC7535] Abley, J., Dickson, B., Kumari, W., and G. Michaelson, "AS112 Redirection Using DNAME", RFC 7535, DOI 10.17487/RFC7535, May 2015, <https://www.rfc-editor.org/info/rfc7535>.

[RFC8023] Thomas, M., Mankin, A., and L. Zhang, "Report from the Workshop and Prize on Root Causes and Mitigation of Name Collisions", RFC 8023, DOI 10.17487/RFC8023, November 2016, <https://www.rfc-editor.org/info/rfc8023>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8590] Gould, J. and K. Feher, "Change Poll Extension for the Extensible Provisioning Protocol (EPP)", RFC 8590, DOI 10.17487/RFC8590, May 2019, <https://www.rfc-editor.org/info/rfc8590>.

[RFC9520] Wessels, D., Carroll, W., and M. Thomas, "Negative Caching of DNS Resolution Failures", RFC 9520, DOI 10.17487/RFC9520, December 2023, <https://www.rfc-editor.org/info/rfc9520>.

[risky-bizness]
Akiwate, G., Savage, S., Voelker, G., and K. Claffy, "Risky BIZness: Risks Derived from Registrar Name Management", November 2021, <https://doi.org/10.1145/3487552.3487816>.

[risky-bizness-irtf]
Akiwate, G., Savage, S., Voelker, G., and K. Claffy, "Risky BIZness: Risks Derived from Registrar Name Management", November 2022, <https://datatracker.ietf.org/doc/slides-115-irtfopen-risky-bizness-risks-derived-from-registrar-name-management/>.

[SAC048] ICANN Security and Stability Advisory Committee, "SSAC Comment on Orphan Glue Records in the Draft Applicant Guidebook", SAC 48, 12 May 2011, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-048-en.pdf>.

[SAC125] ICANN Security and Stability Advisory Committee, "SSAC Report on Registrar Nameserver Management", SAC 125, 9 May 2024, <https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-125-09-05-2024-en.pdf>.

Appendix A. Change Log

This section is to be removed before publishing as an RFC.

This section lists substantial changes to the document as it is being worked on.

00:

1. Initial working group version.

01:

1. Addressed feedback received during the WG adoption request. Re-included text to indicate if approaches have been observed in practice or not.

02:

1. Section 1: Added sentence to bridge between renaming host objects and deletion dilemma.

2. Section 1: Noted that renaming a host object to a name of an external host is an operation that might not be possible to reverse.

3. Section 4: Added mention of "sacrificial" hosts. "ns1.example.org" is a sacrificial host.

4. Section 5.1: Added text to give some more context on "sacrificial" hosts.

5. Section 8: Added text describing DNSSEC risk.

6. Acknowledged Brian Dickson.

03:

1. Added reference to SAC048 in Section 3.1.

2. Added note about minimal risk in Section 3.2.

3. Added context to the best practice recommendations in Section 6.

4. Added "Sacrificial Name Server" to the title of Section 5.1.3.4.

04:

1. Updates to address working group last call feedback:

2. Updated the abstract to note "new possible practices".

3. Split Section 5 into two sections to better identify observed practices and possible practices.

4. Added a specific recommendation to use "sacrificial.invalid" in Section 6.

5. Reorganized practice description sections into subsections of observed practices and potential practices.

05:

1. Move Section 5.2.1.2 into observed practices.

2. Add clearer MUST NOT guidance on Section 5.1.3.1, Section 5.1.3.3, and Section 5.1.4.1.

3. Promoted subsection of potential options to potential practices.

4. Removed redundant explicit delete section.

5. Increased TOC depth.

6. Made section headers clearer, changing "Deletion Observed Practices" and similar to "Observed Practices for Deletion of Hosts," etc.

06:

1. Add reference to SSAC125 complementary document

2. Change recommendations to use MUST language and reference to RFC8244.

3. Rewrite "Allow Explicit Delete of Domain with Restore Capability" text for greater clarity.

07:

1. Consolidate Best Practice Recommendations Section 6

2. Make RFC 3915 normative.

08:

1. Changed subject of Section 6 recommendations from "An EPP server" to "EPP servers and clients."

09:

1. Updated Section 5.1.3.2 for clarity around empty subdomain, to remove confusing/incorrect claim around "valid" DNS name, and to add DNAME mention.

2. Added explanatory sentences to Section 1.

3. Explicitly state that other practices in analysis section are not recommended in Section 6.

4. Clarified sacrificial name server requirements in Section 5.1.3.4.

10:

1. Move SAC048 URL from text to references.

2. Rename Section 5.1.3.4 to explicitly say "dedicated."

3. Remove test/experiment in Section 5.1.4.2.1.

4. Change Section 5.1.3.4 to require authoritative DNS service (previous SHOULD changed to MUST).

Authors' Addresses

Scott Hollenbeck
Verisign Labs
12061 Bluemont Way
Reston, VA 20190
United States of America
Email: shollenbeck@verisign.com
URI: https://www.verisignlabs.com/

William Carroll
Verisign
12061 Bluemont Way
Reston, VA 20190
United States of America
Phone: +1 703 948-3200
Email: wicarroll@verisign.com
URI: https://verisign.com

Gautam Akiwate
Stanford University
450 Jane Stanford Way
Stanford, CA 94305
United States of America
Phone: +1 650 723-2300
Email: gakiwate@cs.stanford.edu
URI: https://cs.stanford.edu/~gakiwate/