

Workgroup: intarea
Internet-Draft:
draft-dkg-intarea-dangerous-labels-00
Published: 6 May 2022
Intended Status: Informational
Expires: 7 November 2022
Authors: D. K. Gillmor
ACLU

Dangerous Labels in DNS and E-mail

Abstract

This document establishes registries that list known security-sensitive labels in the DNS and in e-mail contexts.

It provides references and brief explanations about the risks associated with each known label.

The registries established here offer guidance to the security-minded system administrator, who may not want to permit registration of these labels by untrusted users.

About This Document

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

The latest revision of this draft can be found at <https://dkg.gitlab.io/dangerous-labels/>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-dkg-intarea-dangerous-labels/>.

Discussion of this document takes place on the Internet Area Working Group mailing list (<mailto:intarea@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/intarea/>.

Source for this draft and an issue tracker can be found at <https://gitlab.com/dkg/dangerous-labels>.

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 7 November 2022.

Copyright Notice

Copyright (c) 2022 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](#)
 - [1.1. Requirements Language](#)
- [2. DNS Labels](#)
- [3. E-mail Local Parts](#)
- [4. Security Considerations](#)
- [5. IANA Considerations](#)
- [6. References](#)
 - [6.1. Normative References](#)
 - [6.2. Informative References](#)
- [Appendix A. Acknowledgements](#)
- [Appendix B. Document Considerations](#)
 - [B.1. Other types of labels?](#)
 - [B.2. Document History](#)
- [Author's Address](#)

1. Introduction

The Internet has a few places where seemingly arbitrary labels can show up and be used interchangeably.

Some choices for those labels have surprising or tricky consequences. Reasonable administrators may want to be aware of those labels to avoid an accidental allocation that has security implications.

This document registers a list of labels in DNS and e-mail systems that are known to have a security impact. It is not recommended to create more security-sensitive labels.

Offering a stable registry of these dangerous labels is not an endorsement of the practice of using arbitrary labels in this way. A new protocol that proposes adding a label to this list is encouraged to find a different solution if at all possible.

1.1. Requirements Language

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.

2. DNS Labels

Note that [[RFC8552](#)] defines the use of "underscored" labels which are treated differently than normal DNS labels, and often have security implications. That document also established the IANA registry for "Underscored and Globally Scoped DNS Node Names". That registry takes precedence to the list enumerated here, and any label in that list or with a leading underscore ("_") **MUST NOT** be included in this list.

Below are some normal-looking DNS labels that may grant some form of administrative control over the domain that the are attached to.

They are mostly "leftmost" or least-significant labels (in the sense used in [Section 8](#) of [[RFC8499](#)]), in that if foo were listed here, it would be because granting control over the foo.example.net label (or control over the host pointed to by foo.example.net) to an untrusted party might offer that party some form of administrative control over other parts of example.org.

Note: where "<key-tag>" occurs in [Table 1](#), it indicates any sequence of five or more decimal digits, as described in [[RFC8509](#)].

DNS Label	Rationale and References
mta-sts	Set SMTP transport security policy ([RFC8641])
openpgpkey	Domain-based OpenPGP certificate lookup and verification ([I-D.koch-openpgp-webkey-service])
root-key-sentinel-is-ta-<key-tag>	Indicates which DNSSEC root key is trusted ([RFC8509])

DNS Label	Rationale and References
root-key-sentinel-not-ta-<key-tag>	Indicates which DNSSEC root key is not trusted ([RFC8509])
www	Popular web browsers guess this label (???)

Table 1: Dangerous DNS labels

3. E-mail Local Parts

[Section 3.4.1](#) of [RFC5322] defines the local-part of an e-mail address (the part before the "@" sign) as "domain-dependent". However, allocating some specific local-parts to an untrusted party can have significant security consequences for the domain or other associated resources.

Note that all these labels are expected to be case-insensitive. That is, an administrator restricting registration of a local-part named "admin" **MUST** also apply the same constraint to "Admin" or "ADMIN" or "aDmIn".

[RFC2142] offers some widespread historical practice for common local-parts. The CA/Browser Forum's Baseline Requirements ([CABForum-BR]) constrain how any popular Public Key Infrastructure (PKI) Certification Authority (CA) should confirm domain ownership when verifying by e-mail. The public CAs used by popular web browsers ("web PKI") will adhere to these guidelines, but anyone relying on unusual CAs may still be subject to risk additional labels described here.

E-mail local-part	Rationale and References
abuse	Receive reports of abusive public behavior (Section 2 of [RFC2142])
administrator	PKI Cert Issuance (Section 3.2.2.4.4 of [CABForum-BR])
admin	PKI Cert Issuance (Section 3.2.2.4.4 of [CABForum-BR])
hostmaster	PKI Cert Issuance (Section 3.2.2.4.4 of [CABForum-BR]), DNS zone control (Section 7 of [RFC2142])
info	PKI Cert Issuance (historical, see [VU591120])
is	PKI Cert Issuance (historical, see [VU591120])
it	PKI Cert Issuance (historical, see [VU591120])
noc	Receive reports of network problems (Section 4 of [RFC2142])
postmaster	Receive reports related to SMTP service (Section 5 of [RFC2142]), PKI Cert Issuance (Section 3.2.2.4.4 of [CABForum-BR])
root	Receive system software notifications (???), PKI Cert Issuance (historical, see [VU591120])

E-mail local-part	Rationale and References
security	Receive reports of technical vulnerabilities (Section 4 of [RFC2142])
ssladministrator	PKI Cert Issuance (historical, see [VU591120])
ssladmin	PKI Cert Issuance (historical, see [VU591120])
sslwebmaster	PKI Cert Issuance (historical, see [VU591120])
sysadmin	PKI Cert Issuance (historical, see [VU591120])
webmaster	PKI Cert Issuance (Section 3.2.2.4.4 of [CABForum-BR]), Receive reports related to HTTP service (Section 5 of [RFC2142])
www	Common alias for webmaster (Section 5 of [RFC2142])

Table 2: Dangerous E-mail local-parts

4. Security Considerations

Allowing untrusted parties to allocate names with the labels associated in this document may grant access to administrative capabilities.

The administrator of a DNS or E-mail service that permits any untrusted party to register an arbitrary DNS label or e-mail local-part for their own use **SHOULD** reject attempts to register the labels listed here.

5. IANA Considerations

This document asks IANA to establish two registries, from [Table 1](#) and [Table 2](#).

Note that the DNS table in [Table 1](#) does not include anything that should be handled by the pre-existing "Underscored and Globally Scoped DNS Node Names" registry defined by [\[RFC8552\]](#).

It's not clear how these registries should be updated.

Adding a new security-sensitive entry to either of these tables is likely to be a bad idea, because existing DNS zones and e-mail installations may have already made an allocation of the novel label, and cannot avoid the security implications. For a new protocol that wants to include a label in either registry, there is almost always a better protocol design choice.

Yet, if some common practice permits any form of administrative access to a resource based on control over an arbitrary label, administrators need a central place to keep track of which labels are dangerous.

6. References

6.1. 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>>.
- [RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <<https://www.rfc-editor.org/info/rfc5322>>.
- [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>>.
- [RFC8552] Crocker, D., "Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves", BCP 222, RFC 8552, DOI 10.17487/RFC8552, March 2019, <<https://www.rfc-editor.org/info/rfc8552>>.

6.2. Informative References

- [CABForum-BR] Forum, C., "CA/Browser Forum Baseline Requirements", 23 April 2022, <<https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.8.4.pdf>>.
- [I-D.hoffman-dns-special-labels]
Hoffman, P., "IANA Registry for Special Labels in the DNS", Work in Progress, Internet-Draft, draft-hoffman-dns-special-labels-00, 1 October 2018, <<https://www.ietf.org/archive/id/draft-hoffman-dns-special-labels-00.txt>>.
- [I-D.koch-openpgp-webkey-service]
Koch, W., "OpenPGP Web Key Directory", Work in Progress, Internet-Draft, draft-koch-openpgp-webkey-service-13, 14

November 2021, <<https://www.ietf.org/archive/id/draft-koch-openpgp-webkey-service-13.txt>>.

[RFC2142] Crocker, D., "Mailbox Names for Common Services, Roles and Functions", RFC 2142, DOI 10.17487/RFC2142, May 1997, <<https://www.rfc-editor.org/info/rfc2142>>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <<https://www.rfc-editor.org/info/rfc8499>>.

[RFC8509] Huston, G., Damas, J., and W. Kumari, "A Root Key Trust Anchor Sentinel for DNSSEC", RFC 8509, DOI 10.17487/RFC8509, December 2018, <<https://www.rfc-editor.org/info/rfc8509>>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <<https://www.rfc-editor.org/info/rfc8641>>.

[VU591120] Center, C. C., "Multiple SSL certificate authorities use predefined email addresses as proof of domain ownership", 7 April 2015, <<https://www.kb.cert.org/vuls/id/591120/>>.

Appendix A. Acknowledgements

Many people created these dangerous labels or the authorization processes that rely on them over the years.

Dave Crocker wrote an early list of special e-mail local-parts, from [RFC2142].

Paul Hoffman tried to document a wider survey of special DNS labels (not all security-sensitive) in [I-D.hoffman-dns-special-labels].

Appendix B. Document Considerations

RFC Editor: please remove this section before publication.

B.1. Other types of labels?

This document is limited to leftmost DNS labels and e-mail local-parts because those are the arbitrary labels. There may be other types of arbitrary labels on the Internet with special values that have security implications that the author is not aware of.

B.2. Document History

/No history yet/

Author's Address

Daniel Kahn Gillmor
American Civil Liberties Union
United States of America

Email: dkg@fifthhorseman.net