Abstract

When security risks are discovered by independent security researchers, they often lack the channels to disclose them properly. As a result, security issues may be left unreported. This document defines a standard ("security.txt") to help organizations describe the process for security researchers to follow in order to disclose security vulnerabilities securely.

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 January 16, 2019.

Copyright Notice

Copyright (c) 2018 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 Simplified BSD License text as described in Section 4.e of the IETF Trust Legal Provisions Document.
the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ............................................. 3
  1.1. Motivation and Prior Work ............................ 3
  1.2. Terminology ......................................... 3
2. Note to Readers ........................................... 4
3. The Specification ......................................... 4
  3.1. Scope .................................................. 4
  3.2. Comments ............................................. 5
  3.3. Separate Fields ...................................... 5
  3.4. Field Definitions .................................... 5
    3.4.1. Acknowledgments .................................. 5
    3.4.2. Contact ........................................... 6
    3.4.3. Encryption ....................................... 6
    3.4.4. Hiring ............................................ 7
    3.4.5. Permission ....................................... 7
    3.4.6. Policy ............................................ 8
    3.4.7. Signature ........................................ 8
  3.5. Example of a "security.txt" file ...................... 8
4. Location of the security.txt file ........................ 9
  4.1. Web-based services .................................. 9
  4.2. Filesystems .......................................... 9
  4.3. Internal hosts ...................................... 10
  4.4. Extensibility ....................................... 10
5. File Format Description and ABNF Grammar ................ 10
6. Security considerations .................................. 12
7. IANA Considerations ...................................... 12
  7.1. Well-Known URIs registry ............................ 12
  7.2. Registry for security.txt Header Fields .............. 12
8. Contributors ............................................. 14
9. References ............................................... 15
  9.1. Normative References ................................ 15
  9.2. Informative References .............................. 16
Appendix A. Note to Readers .................................. 17
Appendix B. Document History ................................ 17
  B.1. Since draft-foudil-securitytxt-00 ..................... 17
  B.2. Since draft-foudil-securitytxt-01 ..................... 17
  B.3. Since draft-foudil-securitytxt-02 ..................... 18
  B.4. Since draft-foudil-securitytxt-03 ..................... 18
Authors' Addresses ........................................... 19
1. Introduction

1.1. Motivation and Prior Work

Many security researchers encounter situations where they are unable to responsibly disclose security issues to companies because there is no course of action laid out or no way indicated to contact the owner of a particular resource.

As per section 4 of [RFC2142], there is an existing convention of using the <SECURITY@domain> email address for communications regarding security issues. That convention provides only a single, email-based channel of communication for security issues per domain, and does not provide a way for domain owners to publish information about their security disclosure policies.

There are also contact conventions prescribed for Internet Service Providers (ISPs) in section 2 of [RFC3013], for Computer Security Incident Response Teams (CSIRTs) in section 3.2 of [RFC2350] and for site operators in section 5.2 of [RFC2196]. As per [RFC7485], there is also contact information provided by Regional Internet Registries (RIRs) and domain registries for owners of IP addresses, autonomous system numbers (ASNs) and domain names. However, none of these address the issue of how security researchers can locate disclosure policies and contact information for companies in order to responsibly disclose security issues.

In this document, we define a richer, machine-parsable and more extensible way for companies to communicate information about their security disclosure policies, which is not limited to email and also allows for additional features such as encryption. This standard is designed to help assist with the security disclosure process by making it easier for companies to designate the preferred steps for researchers to take when trying to reach out to them with security issues.

1.2. Terminology

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. Note to Readers

*Note to the RFC Editor:* Please remove this section prior to publication.

Development of this draft takes place on Github at: https://github.com/securitytxt/security-txt

A mailing list is available for discussion at: https://www.freelists.org/list/securitytxt

3. The Specification

This standard defines a text file to be placed in a known location that provides information for security researchers to assist in disclosing security issues.

The file is named "security.txt", and this file SHOULD be placed under the /.well-known/ path ("/.well-known/security.txt") [RFC5785] of a domain name or IP address for web properties. If it is not possible to place the security.txt file in the /.well-known/ path or setup a redirect, web-based services MAY place the file in the top-level path of a given web domain or IP address ("/security.txt") as a fallback option. For web-based services, the instructions MUST be accessible via the Hypertext Transfer Protocol [RFC1945] as a resource of Internet Media Type "text/plain" with the default charset parameter set to "utf-8" per section 4.1.3 of [RFC2046]. For file systems and version control repositories a ".security.txt" file SHOULD be placed in the root directory of a particular file system or source code project.

This text file contains multiple directives with different values. The "directive" is the first part of a field all the way up to the colon ("Contact:"). Directives MUST be case-insensitive. The "value" comes after the directive ("https://example.com/security"). A "field" MUST always consist of a directive and a value ("Contact: https://example.com/security"). A security.txt file can have an unlimited number of fields. It is important to note that you MUST have a separate line for every field. One MUST NOT chain multiple values for a single directive and everything MUST be in a separate field. Unless otherwise indicated in a definition of a particular field, any directive MAY appear multiple times.

3.1. Scope

A "security.txt" file MUST only apply to the domain in the URI used to retrieve it, not to any of its subdomains or parent domains. A "security.txt" file that is found in a file system or version control
repository MUST only apply to the folder or repository in which it is located, and not to any of its parent or sibling folders, or repositories.

Some examples appear below:

# The following only applies to example.com.
https://example.com/.well-known/security.txt

# This only applies to subdomain.example.com.
https://subdomain.example.com/.well-known/security.txt

# This security.txt file applies to IPv4 address of 192.0.2.0.
http://192.0.2.0/.well-known/security.txt

# This security.txt file applies to IPv6 address of 2001:db8:8:4::2.
http://[2001:db8:8:4::2]/.well-known/security.txt

# This security.txt file applies to the /example/folder1 directory.
/example/folder1/security.txt

3.2. Comments

Any line beginning with the "#" (%x30) symbol MUST be interpreted as a comment.

Example:

# This is a comment.

You MAY use one or more comments as descriptive text immediately before the field. Parsers SHOULD associate the comments with the respective field.

3.3. Separate Fields

A separate line is REQUIRED for every new value and field. You MUST NOT chain everything into a single field. Every line MUST end either with a carriage return and line feed characters (CRLF / %x0D %x0A) or just a line feed character (LF / %x0A).

3.4. Field Definitions

3.4.1. Acknowledgments

This directive allows you to link to a page where security researchers are recognized for their reports. The page being linked
to SHOULD list individuals or companies that disclosed security vulnerabilities and worked with you to remediate the issue.

Example:

Acknowledgments: https://example.com/hall-of-fame.html

Example security acknowledgments page:

We would like to thank the following researchers:

(2017-04-15) Frank Denis - Reflected cross-site scripting
(2017-01-02) Alice Quinn - SQL injection
(2016-12-24) John Buchner - Stored cross-site scripting
(2016-06-10) Anna Richmond - A server configuration issue

3.4.2. Contact

This directive allows you to provide an address that researchers SHOULD use for reporting security issues. The value MAY be an email address, a phone number and/or a contact page with more information. The "Contact:" directive MUST always be present in a security.txt file. If this directive indicates a web URL, then it MUST be begin with "https://". Security email addresses SHOULD use the conventions defined in section 4 of [RFC2142], but there is no requirement for this directive to be an email address.

The value MUST follow the general syntax described in [RFC3986]. This means that "mailto" and "tel" URI schemes MUST be used when specifying email addresses and telephone numbers.

The precedence SHOULD be in listed order. The first field is the preferred method of contact. In the example below, the e-mail address is the preferred method of contact.

Contact: mailto:security@example.com
Contact: tel:+1-201-555-0123
Contact: https://example.com/security-contact.html

3.4.3. Encryption

This directive allows you to point to an encryption key that security researchers SHOULD use for encrypted communication. You MUST NOT directly add your key to the field, instead the value of this field MUST be a URI pointing to a location where the key can be retrieved from. If this directive indicates a web URL, then it MUST be begin with "https://".
When it comes to verifying the authenticity of the key, it is always the security researcher's responsibility to make sure the key being specified is indeed one they trust. Researchers MUST NOT assume that this key is used to generate the signature file referenced in Section 3.4.7.

Example of a PGP key available from a web server:

Encryption: https://example.com/pgp-key.txt

Example of a PGP key available from an OPENPGPKEY DNS:

Encryption: dns:5d2d37ab76d47d36._openpgpkey.example.com?type=OPENPGPKEY

Example of a PGP key being referenced by its fingerprint:

Encryption: openpgp4fpr:5f2de5521c63a801ab59ccb603d49de44b29100f

3.4.4. Hiring

The "Hiring" directive is used for linking to the vendor's security-related job positions. If this directive indicates a web URL, then it SHOULD be begin with "https://".

Hiring: https://example.com/jobs.html

3.4.5. Permission

The presence of the "Permission" directive is used to indicate to security researchers that they MUST NOT perform any kind of testing against the resource hosting the "security.txt" file. This field MUST have a value which is REQUIRED to be set to the string "none". Other values MUST NOT be used. This field MUST NOT appear more than once.

The absence of the "Permission" directive or the use of any other value other than "none" for this directive MUST NOT be interpreted by researchers as being granted permission to test the resource. Additionally, the presence or absence of this directive MUST NOT be interpreted as having any legal value.

Example:

Permission: none
3.4.6. Policy

This directive allows you to link to where your security policy and/or disclosure policy is located. This can help security researchers understand what you are looking for and how to report security vulnerabilities. If this directive indicates a web URL, then it SHOULD begin with "https://".

Example:

Policy: https://example.com/security-policy.html

3.4.7. Signature

This directive allows you to specify a full URI (as per [RFC3986]) of an external signature file that can be used to check the authenticity of a "security.txt" file. External signature files SHOULD be named "security.txt.sig" and SHOULD be placed under the /.well-known/ path ("/.well-known/security.txt.sig"). If this directive indicates a web URL, then it MUST be begin with "https://". This directive MUST NOT appear more than once.

It is RECOMMENDED to implementors that this directive be always used.

When it comes to verifying the authenticity of the file, it is always the security researcher's responsibility to make sure the key being specified is indeed one they trust.

Here is an example of an external signature file.

Signature: https://example.com/.well-known/security.txt.sig

3.5. Example of a "security.txt" file

# Our security address
Contact: mailto:security@example.com

# Our PGP key
Encryption: https://example.com/pgp-key.txt

# Our security policy
Policy: https://example.com/security-policy.html

# Our security acknowledgments page
Acknowledgments: https://example.com/hall-of-fame.html

# Verify this security.txt file
Signature: https://example.com/.well-known/security.txt.sig
4. **Location of the security.txt file**

- **External**
  - Default
  - Redirect
  - /well-known/security.txt <--- /security.txt
  - +-----------------------------+          +-----------------+  |
  - |                             |          |                 |  |
  - | /well-known/security.txt    <--------+ /security.txt |  |
  - |                             |          |                 |  |
  - +-----------------------------+          +-----------------+  |

- **Internal**
  - +------------------------+
  - |                        |
  - |  /.security.txt         |
  - |                        |
  - | +------------------------|

**4.1. Web-based services**

Web-based services SHOULD place the security.txt file under the /.well-known/ path; e.g. https://example.com/.well-known/security.txt. A security.txt file located under the top-level path SHOULD either redirect (as per section 6.4 of [RFC7231]) to the security.txt file under the /.well-known/ path or be used as a fallback.

**4.2. Filesystems**

File systems SHOULD place the security.txt file under the root directory; e.g., /.security.txt, C:.security.txt.

```
user:/$ l
.security.txt
example-directory-1/
example-directory-2/
example-directory-3/
exanple-file
```
4.3. Internal hosts

A .security.txt file SHOULD be placed in the root directory of an internal host.

4.4. Extensibility

Like many other formats and protocols, this format may need to be extended over time to fit the ever-changing landscape of the Internet. Therefore, extensibility is provided via an IANA registry for directives as defined in Section 7.2. Any directives registered via that process MUST be considered optional. To encourage extensibility and interoperability, implementors MUST ignore any fields they do not explicitly support.

5. File Format Description and ABNF Grammar

The expected file format of the security.txt file is plain text (MIME type "text/plain") as defined in section 4.1.3 of [RFC2046] and is encoded using UTF-8 [RFC3629] in Net-Unicode form [RFC5198].

The following is an ABNF definition of the security.txt format, using the conventions defined in [RFC5234] and [RFC5322].
body = *line (permission-field eol) (signature-field eol)
*line

line = *1(field / comment) eol

eol = *WSP [CR] LF

field = acknowledgments-field /
        contact-field /
        encryption-field /
        hiring-field /
        policy-field /
        ext-field

fs = ":"

comment = "#" *(WSP / VCHAR / %xA0-%E007F)

acknowledgments-field = "Acknowledgments" fs SP uri

contact-field = "Contact" fs SP (email / uri / phone)

email = <Email address as per {{RFC5322}}>

phone = "+" *1(DIGIT / "-" / "(" / ")" / SP)

uri = <URI as per {{RFC3986}}>

encryption-field = "Encryption" fs SP uri

hiring-field = "Hiring" fs SP uri

permission-field = "Permission" fs SP "none"

policy-field = "Policy" fs SP uri

signature-field = "Signature" fs SP uri

ext-field = field-name fs SP unstructured

field-name = <as per section 3.6.8 of {{RFC5322}}>

unstructured = <as per section 3.2.5 of {{RFC5322}}>

"ext-field" refers to extension fields, which are discussed in

Section 4.4
6. Security considerations

Organizations creating security.txt files will need to consider several security-related issues. These include exposure to sensitive information and attacks where limited access to a server could grant the ability to modify the contents of the security.txt file or affect how it is served. Organizations SHOULD also monitor their security.txt files regularly to detect tampering. Organizations SHOULD also ensure that any resources such as web pages, email addresses and telephone numbers references by a "security.txt" file are kept current, are accessible and controlled by the organization, and are kept secure.

To ensure the authenticity of the security.txt file, organizations SHOULD sign the file and include the signature using the "Signature" directive (Section 3.4.7). As stated in Section 3.4.3 and Section 3.4.7, both encryption keys and external signature files MUST be loaded over HTTPS.

Websites SHOULD reserve the security.txt namespace to ensure no third-party can create a page with the "security.txt" name.

7. IANA Considerations

example.com is used in this document following the uses indicated in [RFC2606].

192.0.2.0 and 2001:db8:8:4::2 are used in this document following the uses indicated in [RFC6890].

7.1. Well-Known URIs registry

The "Well-Known URIs" registry should be updated with the following additional values (using the template from [RFC5785]):

URI suffix: security.txt

URI suffix: security.txt.sig

Change controller: IETF

Specification document(s): this document

7.2. Registry for security.txt Header Fields

IANA is requested to create the "security.txt Header Fields" registry in accordance with [RFC8126]. This registry will contain header fields for use in security.txt files, defined by this specification.
New registrations or updates MUST be published in accordance with the "Expert Review" guidelines as described in section 4.5 of [RFC8126]. Any new field thus registered is considered optional by this specification unless a new version of this specification is published.

New registrations and updates MUST contain the following information:

1. Name of the field being registered or updated
2. Short description of the field
3. Whether the field can appear more than once
4. The document in which the specification of the field is published
5. New or updated status, which MUST be one of: current: The field is in current use deprecated: The field is in current use, but its use is discouraged historic: The field is no longer in current use

An update may make a notation on an existing registration indicating that a registered field is historical or deprecated if appropriate.

The initial registry contains these values:
8. Contributors

The authors would like to acknowledge the help provided during the development of this document by Tom Hudson, Joel Margolis, Jobert Abma, Gerben Janssen van Doorn, Austin Heap, Justin Calmus, and Casey Ellis.
The authors would also like to acknowledge the feedback provided by multiple members of IETF's SAAG and SEC-DISPATCH lists.

9. References

9.1. Normative References


9.2. Informative References


Appendix A. Note to Readers

*Note to the RFC Editor:* Please remove this section prior to publication.

Development of this draft takes place on Github at https://github.com/securitytxt/security-txt

Appendix B. Document History

*Note to the RFC Editor:* Please remove this section prior to publication.

B.1. Since draft-foudil-securitytxt-00

- Moved to use IETF's markdown tools for draft updates
- Added table of contents and a fuller list of references
- Moved file to .well-known URI and added IANA registration (#3)
- Added extensibility with an IANA registry for fields (#34)
- Added text explaining relationship to RFC 2142 / security@ email address (#25)
- Scope expanded to include internal hosts, domains, IP addresses and file systems
- Support for digital signatures added (#19)

The full list of changes can be viewed via the IETF document tracker: https://tools.ietf.org/html/draft-foudil-securitytxt-01

B.2. Since draft-foudil-securitytxt-01

- Added appendix with pointer to Github and document history
- Added external signature file to the well known URI registry (#59)
- Added policy field (#53)
- Added diagram explaining the location of the file on public vs. internal systems
- Added recommendation that external signature files should use HTTPS (#55)
o Added recommendation that organizations should monitor their security.txt files (#14)

The full list of changes can be viewed via the IETF document tracker: https://tools.ietf.org/html/draft-foudil-securitytxt-02

B.3. Since draft-foudil-securitytxt-02

  o Use "mailto" and "tel" (#62)
  o Fix typo in the "Example" section (#64)
  o Clarified that the root directory is a fall back option (#72)
  o Defined content-type for the response (#68)
  o Clarify the scope of the security.txt file (#69)
  o Cleaning up text based on the NITS tools suggestions (#82)
  o Added clarification for newline values
  o Clarified the encryption field language, added examples of DNS-stored encryption keys (#28 and #94)
  o Added "Hiring" field

B.4. Since draft-foudil-securitytxt-03

  o Added "Hiring" field to the registry section
  o Added an encryption example using a PGP fingerprint (#107)
  o Added reference to the mailing list (#111)
  o Added a section referencing related work (#113)
  o Fixes for idnits (#82)
  o Changing some references to informative instead of normative
  o Adding "Permission" field (#30)
  o Fixing remaining ABNF issues (#83)
  o Additional editorial changes and edits
Full list of changes can be viewed via the IETF document tracker: https://tools.ietf.org/html/draft-foudil-securitytxt

Authors' Addresses

Edwin Foudil
Email: contact@edoverflow.com

Yakov Shafranovich
Nightwatch Cybersecurity
Email: yakov+ietf@nightwatchcybersecurity.com