Stream: Internet Engineering Task Force (IETF)
RFC: 9116
Category: Informational
Published: April 2022
ISSN: 2070-1721
Authors: E. Foudil Y. Shafranovich
Nightwatch Cybersecurity

RFC 9116
A File Format to Aid in Security Vulnerability Disclosure

Abstract

When security vulnerabilities are discovered by researchers, proper reporting channels are often lacking. As a result, vulnerabilities may be left unreported. This document defines a machine-parsable format ("security.txt") to help organizations describe their vulnerability disclosure practices to make it easier for researchers to report vulnerabilities.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9116.

Copyright Notice

Table of Contents

1. Introduction

1.1. Motivation, Prior Work, and Scope

Many security researchers encounter situations where they are unable to report security vulnerabilities to organizations because there are no reporting channels to contact the owner of a particular resource, and no information is available about the vulnerability disclosure practices of such owner.

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 per domain and does not provide a way for domain owners to publish information about their security disclosure practices.

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 tackle the issue of how security researchers can locate contact information and vulnerability disclosure practices for organizations in order to report vulnerabilities.

In this document, we define a richer, machine-parsable, and more extensible way for organizations to communicate information about their security disclosure practices and ways to contact them. Other details of vulnerability disclosure are outside the scope of this document. Readers are encouraged to consult other documents such as [ISO.29147.2018] or [CERT.CVD].

As per [CERT.CVD], "vulnerability response" refers to reports of product vulnerabilities, which is related to but distinct from reports of network intrusions and compromised websites ("incident response"). The mechanism defined in this document is intended to be used for the former ("vulnerability response"). If implementors want to utilize this mechanism for incident response, they should be aware of additional security considerations discussed in Section 5.1.

The "security.txt" file is intended to be complementary and not a substitute or replacement for other public resources maintained by organizations regarding their security disclosure practices.

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.

The term "researcher" corresponds to the terms "finder" and "reporter" in [ISO.29147.2018] and [CERT.CVD]. The term "organization" corresponds to the term "vendor" in [ISO.29147.2018] and [CERT.CVD].

The term "implementors" includes all parties involved in the vulnerability disclosure process.

2. The Specification

This document defines a text file to be placed in a known location that provides information about vulnerability disclosure practices of a particular organization. The format of this file is machine parsable and **MUST** follow the ABNF grammar defined in Section 4. This file is intended to help security researchers when disclosing security vulnerabilities.

By convention, the file is named "security.txt". The location and scope are described in Section 3.

This text file contains multiple fields with different values. A field contains a "name", which is the first part of a field all the way up to the colon (for example: "Contact:") and follows the syntax defined for "field-name" in Section 3.6.8 of [RFC5322]. Field names are case insensitive (as per Section 2.3 of [RFC5234]). The "value" comes after the field name (for example: "mailto:security@example.com") and follows the syntax defined for "unstructured" in Section 3.2.5 of [RFC5322]. The file **MAY** also contain blank lines.

A field **MUST** always consist of a name and a value (for example: "Contact: mailto:security@example.com"). A "security.txt" file can have an unlimited number of fields. Each field **MUST** appear on its own line. Unless otherwise specified by the field definition, multiple values **MUST NOT** be chained together for a single field. Unless otherwise indicated in a definition of a particular field, a field **MAY** appear multiple times.

Implementors should be aware that some of the fields may contain URIs using percent-encoding (as per Section 2.1 of [RFC3986]).

2.1. Comments

Any line beginning with the "#" (%x23) symbol **MUST** be interpreted as a comment. The content of the comment may contain any ASCII or Unicode characters in the %x21-7E and %x80-FFFFF ranges plus the tab (%x09) and space (%x20) characters.

Example:

```
# This is a comment.
```

2.2. Line Separator

Every line **MUST** end with either a carriage return and line feed characters (CRLF / %x0D %x0A) or just a line feed character (LF / %x0A).

2.3. Digital Signature

It is **RECOMMENDED** that a "security.txt" file be digitally signed using an OpenPGP cleartext signature as described in Section 7 of [RFC4880]. When digital signatures are used, it is also **RECOMMENDED** that organizations use the "Canonical" field (as per Section 2.5.2), thus allowing the digital signature to authenticate the location of the file.

When it comes to verifying the key used to generate the signature, it is always the security researcher's responsibility to make sure the key being used is indeed one they trust.

2.4. Extensibility

Like many other formats and protocols, this format may need to be changed over time to fit the ever-changing landscape of the Internet. Therefore, extensibility is provided via an IANA registry for fields as defined in Section 6.2. Any fields registered via that process **MUST** be considered optional. To encourage extensibility and interoperability, researchers **MUST** ignore any fields they do not explicitly support.

In general, implementors should "be conservative in what you do, be liberal in what you accept from others" (as per [RFC0793]).

2.5. Field Definitions

Unless otherwise stated, all fields **MUST** be considered optional.

2.5.1. Acknowledgments

The "Acknowledgments" field indicates a link to a page where security researchers are recognized for their reports. The page being referenced should list security researchers that reported security vulnerabilities and collaborated to remediate them. Organizations should be careful to limit the vulnerability information being published in order to prevent future attacks.

If this field indicates a web URI, then it **MUST** begin with "https://" (as per Section 2.7.2 of [RFC7230]).

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
```

2.5.2. Canonical

The "Canonical" field indicates the canonical URIs where the "security.txt" file is located, which is usually something like "https://example.com/.well-known/security.txt". If this field indicates a web URI, then it **MUST** begin with "https://" (as per Section 2.7.2 of [RFC7230]).

While this field indicates that a "security.txt" retrieved from a given URI is intended to apply to that URI, it **MUST NOT** be interpreted to apply to all canonical URIs listed within the file. Researchers **SHOULD** use an additional trust mechanism such as a digital signature (as per Section 2.3) to make the determination that a particular canonical URI is applicable.

If this field appears within a "security.txt" file and the URI used to retrieve that file is not listed within any canonical fields, then the contents of the file **SHOULD NOT** be trusted.

```
Canonical: https://www.example.com/.well-known/security.txt
Canonical: https://someserver.example.com/.well-known/security.txt
```

2.5.3. Contact

The "Contact" field indicates a method that researchers should use for reporting security vulnerabilities such as an email address, a phone number, and/or a web page with contact information. This field **MUST** always be present in a "security.txt" file. If this field indicates a web URI, then it **MUST** begin with "https://" (as per Section 2.7.2 of [RFC7230]). Security email addresses should use the conventions defined in Section 4 of [RFC2142].

The value **MUST** follow the URI syntax described in Section 3 of [RFC3986]. This means that "mailto" and "tel" URI schemes must be used when specifying email addresses and telephone numbers, as defined in [RFC6068] and [RFC3966]. When the value of this field is an email address, it is **RECOMMENDED** that encryption be used (as per Section 2.5.4).

These **SHOULD** be listed in order of preference, with the first occurrence being the preferred method of contact, the second occurrence being the second most preferred method of contact, etc. In the example below, the first email address ("security@example.com") is the preferred method of contact.

```
Contact: mailto:security@example.com
Contact: mailto:security%2Buri%2Bencoded@example.com
Contact: tel:+1-201-555-0123
Contact: https://example.com/security-contact.html
```

2.5.4. Encryption

The "Encryption" field indicates an encryption key that security researchers should use for encrypted communication. Keys **MUST NOT** appear in this field. Instead, the value of this field **MUST** be a URI pointing to a location where the key can be retrieved. If this field indicates a web URI, then it **MUST** begin with "https://" (as per Section 2.7.2 of [RFC7230]).

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 digital signature referenced in Section 2.3.

Example of an OpenPGP key available from a web server:

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

Example of an OpenPGP key available from an OPENPGPKEY DNS record:

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

Example of an OpenPGP key being referenced by its fingerprint:

```
Encryption: openpgp4fpr:5f2de5521c63a801ab59ccb603d49de44b29100f
```

2.5.5. Expires

The "Expires" field indicates the date and time after which the data contained in the "security.txt" file is considered stale and should not be used (as per Section 5.3). The value of this field is formatted according to the Internet profiles of [ISO.8601-1] and [ISO.8601-2] as defined in [RFC3339]. It is **RECOMMENDED** that the value of this field be less than a year into the future to avoid staleness.

This field **MUST** always be present and **MUST NOT** appear more than once.

```
Expires: 2021-12-31T18:37:07z
```

2.5.6. Hiring

The "Hiring" field is used for linking to the vendor's security-related job positions. If this field indicates a web URI, then it **MUST** begin with "https://" (as per Section 2.7.2 of [RFC7230]).

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

2.5.7. Policy

The "Policy" field indicates a link to where the vulnerability disclosure policy is located. This can help security researchers understand the organization's vulnerability reporting practices. If this field indicates a web URI, then it **MUST** begin with "https://" (as per Section 2.7.2 of [RFC7230]).

Example:

```
Policy: https://example.com/disclosure-policy.html
```

2.5.8. Preferred-Languages

The "Preferred-Languages" field can be used to indicate a set of natural languages that are preferred when submitting security reports. This set **MAY** list multiple values, separated by commas. If this field is included, then at least one value **MUST** be listed. The values within this set are language tags (as defined in [RFC5646]). If this field is absent, security researchers may assume that English is the language to be used (as per Section 4.5 of [RFC2277]).

The order in which they appear is not an indication of priority; the listed languages are intended to have equal priority.

This field **MUST NOT** appear more than once.

Example (English, Spanish and French):

```
Preferred-Languages: en, es, fr
```

2.6. Example of an Unsigned "security.txt" File

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

# Our OpenPGP 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

Expires: 2021-12-31T18:37:07z
```

2.7. Example of a Signed "security.txt" File

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

# Canonical URI
Canonical: https://example.com/.well-known/security.txt

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

# Our OpenPGP 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

Expires: 2021-12-31T18:37:07z
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.2

[signature]
-----END PGP SIGNATURE-----
```

3. Location of the security.txt File

For web-based services, organizations **MUST** place the "security.txt" file under the "/.well-known/" path, e.g., https://example.com/.well-known/security.txt as per [RFC8615] of a domain name or IP address. For legacy compatibility, a "security.txt" file might be placed at the top-level path or redirect (as per Section 6.4 of [RFC7231]) to the "security.txt" file under the "/.well-known/" path. If a "security.txt" file is present in both locations, the one in the "/.well-known/" path **MUST** be used.

The file **MUST** be accessed via HTTP 1.0 or a higher version, and the file access **MUST** use the "https" scheme (as per Section 2.7.2 of [RFC7230]). It **MUST** have a Content-Type of "text/plain" with the default charset parameter set to "utf-8" (as per Section 4.1.3 of [RFC2046]).

Retrieval of "security.txt" files and resources indicated within such files may result in a redirect (as per Section 6.4 of [RFC7231]). Researchers should perform additional analysis (as per Section 5.2) to make sure these redirects are not malicious or pointing to resources controlled by an attacker.

3.1. Scope of the File

A "security.txt" file **MUST** only apply to the domain or IP address in the URI used to retrieve it, not to any of its subdomains or parent domains. A "security.txt" file **MAY** also apply to products and services provided by the organization publishing the file.

As per Section 1.1, this specification is intended for a vulnerability response. If implementors want to use this for an incident response, they should be aware of additional security considerations discussed in Section 5.1.

Organizations **SHOULD** use the policy directive (as per Section 2.5.7) to provide additional details regarding the scope and details of their vulnerability disclosure process.

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.
https://192.0.2.0/.well-known/security.txt

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

4. File Format Description and ABNF Grammar

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

The format of this file **MUST** follow the ABNF definition below (which incorporates the core ABNF rules from [RFC5234] and uses the case-sensitive string support from [RFC7405]).

```
body             =  signed / unsigned

unsigned       =  *line (contact-field eol) ; one or more required
                  *line (expires-field eol) ; exactly one required
                  *line [lang-field eol] *line ; exactly one optional
                  ; order of fields within the file is not important
                  ; except that if contact-field appears more
                  ; than once, the order of those indicates
                  ; priority (see Section 3.5.3)

; signed is the production that should match the OpenPGP clearsigned
; document
signed           =  cleartext-header
                    1*(hash-header)
                    CRLF
                    cleartext
                    signature

cleartext-header =  %s"-----BEGIN PGP SIGNED MESSAGE-----" CRLF

hash-header      =  %s"Hash: " hash-alg *("," hash-alg) CRLF

hash-alg         =  token
                      ; imported from RFC 2045; see RFC 4880 Section
                      ; 10.3.3 for a pointer to the registry of
                      ; valid values

;cleartext       =  1*( UTF8-octets [CR] LF)
                      ; dash-escaped per RFC 4880 Section 7.1

cleartext        =  *((line-dash / line-from / line-nodash) [CR] LF)

line-dash        =  ("- ") "-" *UTF8-char-not-cr
                       ; MUST include initial "- "

line-from        =  ["- "] "From " *UTF8-char-not-cr
                      ; SHOULD include initial "- "

line-nodash      =  ["- "] *UTF8-char-not-cr
                      ; MAY include initial "- "

UTF8-char-not-dash =  UTF8-1-not-dash / UTF8-2 / UTF8-3 / UTF8-4
UTF8-1-not-dash  =  %x00-2C / %x2E-7F
UTF8-char-not-cr =  UTF8-1-not-cr / UTF8-2 / UTF8-3 / UTF8-4
UTF8-1-not-cr    =  %x00-0C / %x0E-7F
```

```
; UTF8 rules from RFC 3629
UTF8-octets      =  *( UTF8-char )
UTF8-char        =  UTF8-1 / UTF8-2 / UTF8-3 / UTF8-4
UTF8-1           =  %x00-7F
UTF8-2           =  %xC2-DF UTF8-tail
UTF8-3           =  %xE0 %xA0-BF UTF8-tail / %xE1-EC 2( UTF8-tail ) /
                    %xED %x80-9F UTF8-tail / %xEE-EF 2( UTF8-tail )
UTF8-4           =  %xF0 %x90-BF 2( UTF8-tail ) /
                    %xF1-F3 3( UTF8-tail ) /
                    %xF4 %x80-8F 2( UTF8-tail )
UTF8-tail        =  %x80-BF

signature        =  armor-header
                    armor-keys
                    CRLF
                    signature-data
                    armor-tail

armor-header     =  %s"-----BEGIN PGP SIGNATURE-----" CRLF

armor-keys       =  *(token ": " *( VCHAR / WSP ) CRLF)
                      ; Armor Header Keys from RFC 4880

armor-tail       =  %s"-----END PGP SIGNATURE-----" CRLF

signature-data   =  1*(1*(ALPHA / DIGIT / "=" / "+" / "/") CRLF)
                      ; base64; see RFC 4648
                      ; includes RFC 4880 checksum

line             =  [ (field / comment) ] eol

eol              =  *WSP [CR] LF

field            =  ; optional fields
                    ack-field /
                    can-field /
                    contact-field / ; optional repeated instances
                    encryption-field /
                    hiring-field /
                    policy-field /
                    ext-field

fs               =  ":"

comment          =  "#" *(WSP / VCHAR / %x80-FFFFF)

ack-field        =  "Acknowledgments" fs SP uri

can-field        =  "Canonical" fs SP uri

contact-field    =  "Contact" fs SP uri

expires-field    =  "Expires" fs SP date-time

encryption-field =  "Encryption" fs SP uri

hiring-field     =  "Hiring" fs SP uri
```

```
lang-field       =  "Preferred-Languages" fs SP lang-values

policy-field     =  "Policy" fs SP uri

date-time        =  < imported from Section 5.6 of [RFC3339] >

lang-tag         =  < Language-Tag from Section 2.1 of [RFC5646] >

lang-values      =  lang-tag *(*WSP "," *WSP lang-tag)

uri              =  < URI as per Section 3 of [RFC3986] >

ext-field        =  field-name fs SP unstructured

field-name       =  < imported from Section 3.6.8 of [RFC5322] >

unstructured     =  < imported from Section 3.2.5 of [RFC5322] >

token            =  < imported from Section 5.1 of [RFC2045] >

ALPHA            =  %x41-5A / %x61-7A   ; A-Z / a-z

BIT              =  "0" / "1"

CHAR             =  %x01-7F
                      ; any 7-bit US-ASCII character,
                      ;  excluding NUL

CR               =  %x0D
                      ; carriage return

CRLF             =  CR LF
                      ; Internet standard newline

CTL              =  %x00-1F / %x7F
                      ; controls

DIGIT            =  %x30-39
                      ; 0-9

DQUOTE           =  %x22
                      ; " (Double Quote)

HEXDIG           =  DIGIT / "A" / "B" / "C" / "D" / "E" / "F"

HTAB             =  %x09
                      ; horizontal tab

LF               =  %x0A
                      ; linefeed

LWSP             =  *(WSP / CRLF WSP)
                      ; Use of this linear-white-space rule
                      ;  permits lines containing only white
                      ;  space that are no longer legal in
                      ;  mail headers and have caused
                      ;  interoperability problems in other
```

```
                        ;  contexts.
                        ; Do not use when defining mail
                        ;  headers and use with caution in
                        ;  other contexts.

OCTET           =  %x00-FF
                     ; 8 bits of data

SP              =  %x20

VCHAR           =  %x21-7E
                     ; visible (printing) characters

WSP             =  SP / HTAB
                     ; white space
```

"ext-field" refers to extension fields, which are discussed in Section 2.4.

5. Security Considerations

Because of the use of URIs and well-known resources, security considerations of [RFC3986] and [RFC8615] apply here, in addition to the considerations outlined below.

5.1. Compromised Files and Incident Response

An attacker that has compromised a website is able to compromise the "security.txt" file as well or set up a redirect to their own site. This can result in security reports not being received by the organization or being sent to the attacker.

To protect against this, organizations should use the "Canonical" field to indicate the locations of the file (as per Section 2.5.2), digitally sign their "security.txt" files (as per Section 2.3), and regularly monitor the file and the referenced resources to detect tampering.

Security researchers should validate the "security.txt" file, including verifying the digital signature and checking any available historical records before using the information contained in the file. If the "security.txt" file looks suspicious or compromised, it should not be used.

While it is not recommended, implementors may choose to use the information published within a "security.txt" file for an incident response. In such cases, extreme caution should be taken before trusting such information, since it may have been compromised by an attacker. Researchers should use additional methods to verify such data including out-of-band verification of the Pretty Good Privacy (PGP) signature, DNSSEC-based approaches, etc.

5.2. Redirects

When retrieving the file and any resources referenced in the file, researchers should record any redirects since they can lead to a different domain or IP address controlled by an attacker. Further inspection of such redirects is recommended before using the information contained within the file.

5.3. Incorrect or Stale Information

If information and resources referenced in a "security.txt" file are incorrect or not kept up to date, this can result in security reports not being received by the organization or sent to incorrect contacts, thus exposing possible security issues to third parties. Not having a "security.txt" file may be preferable to having stale information in this file. Organizations must use the "Expires" field (see Section 2.5.5) to indicate to researchers when the data in the file is no longer valid.

Organizations should ensure that information in this file and any referenced resources such as web pages, email addresses, and telephone numbers are kept current, are accessible, are controlled by the organization, and are kept secure.

5.4. Intentionally Malformed Files, Resources, and Reports

It is possible for compromised or malicious sites to create files that are extraordinarily large or otherwise malformed in an attempt to discover or exploit weaknesses in the parsing code. Researchers should make sure that any such code is robust against large or malformed files and fields, and they may choose to have the code not parse files larger than 32 KBs, those with fields longer than 2,048 characters, or those containing more than 1,000 lines. The ABNF grammar (as defined in Section 4) can also be used as a way to verify these files.

The same concerns apply to any other resources referenced within "security.txt" files, as well as any security reports received as a result of publishing this file. Such resources and reports may be hostile, malformed, or malicious.

5.5. No Implied Permission for Testing

The presence of a "security.txt" file might be interpreted by researchers as providing permission to do security testing against the domain or IP address where it is published or against products and services provided by the organization publishing the file. This might result in increased testing against an organization by researchers. On the other hand, a decision not to publish a "security.txt" file might be interpreted by the organization operating that website to be a way to signal to researchers that permission to test that particular site or project is denied. This might result in pushback against researchers reporting security issues to that organization.

Therefore, researchers shouldn't assume that the presence or absence of a "security.txt" file grants or denies permission for security testing. Any such permission may be indicated in the company's vulnerability disclosure policy (as per Section 2.5.7) or a new field (as per Section 2.4).

5.6. Multi-User Environments

In multi-user / multi-tenant environments, it may be possible for a user to take over the location of the "security.txt" file. Organizations should reserve the "security.txt" namespace at the root to ensure no third party can create a page with the "security.txt" AND "/.well-known/security.txt" names.

5.7. Protecting Data in Transit

To protect a "security.txt" file from being tampered with in transit, implementors **MUST** use HTTPS (as per Section 2.7.2 of [RFC7230]) when serving the file itself and for retrieval of any web URIs referenced in it (except when otherwise noted in this specification). As part of the TLS handshake, researchers should validate the provided X.509 certificate in accordance with [RFC6125] and the following considerations:

- Matching is performed only against the DNS-ID identifiers.
- DNS domain names in server certificates **MAY** contain the wildcard character '*' as the complete leftmost label within the identifier.

The certificate may also be checked for revocation via the Online Certificate Status Protocol (OCSP) [RFC6960], certificate revocation lists (CRLs), or similar mechanisms.

In cases where the "security.txt" file cannot be served via HTTPS (such as localhost) or is being served with an invalid certificate, additional human validation is recommended since the contents may have been modified while in transit.

As an additional layer of protection, it is also recommended that organizations digitally sign their "security.txt" file with OpenPGP (as per Section 2.3). Also, to protect security reports from being tampered with or observed while in transit, organizations should specify encryption keys (as per Section 2.5.4) unless HTTPS is being used for report submission.

However, the determination of validity of such keys is out of scope for this specification. Security researchers need to establish other secure means to verify them.

5.8. Spam and Spurious Reports

Similar to concerns in [RFC2142], denial-of-service attacks via spam reports would become easier once a "security.txt" file is published by an organization. In addition, there is an increased likelihood of reports being sent in an automated fashion and/or as a result of automated scans without human analysis. Attackers can also use this file as a way to spam unrelated third parties by listing their resources and/or contact information.

Organizations need to weigh the advantages of publishing this file versus the possible disadvantages and increased resources required to analyze security reports.

Security researchers should review all information within the "security.txt" file before submitting reports in an automated fashion or reports resulting from automated scans.

6. IANA Considerations

Implementors should be aware that any resources referenced within a "security.txt" file **MUST NOT** point to the Well-Known URIs namespace unless they are registered with IANA (as per [RFC8615]).

6.1. Well-Known URIs Registry

IANA has updated the "Well-Known URIs" registry with the following additional values (using the template from [RFC8615]):

URI suffix: security.txt
Change controller: IETF
Specification document(s): RFC 9116
Status: permanent

6.2. Registry for security.txt Fields

IANA has created the "security.txt Fields" registry in accordance with [RFC8126]. This registry contains 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 Sections 4.5 and 5 of [RFC8126]. Any new field thus registered is considered optional by this specification unless a new version of this specification is published.

Designated experts should determine whether a proposed registration or update provides value to organizations and researchers using this format and makes sense in the context of industry-accepted vulnerability disclosure processes such as [ISO.29147.2018] and [CERT.CVD].

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. New or updated status, which **MUST** be one of the following:

   current: The field is in current use.
   deprecated: The field has been in use, but new usage is discouraged.
   historic: The field is no longer in current use.
5. Change controller
6. The document in which the specification of the field is published (if available)

Existing registrations may be marked historic or deprecated, as appropriate, by a future update to this document.

The initial registry contains these values:

Field Name: Acknowledgments
Description: link to page where security researchers are recognized
Multiple Appearances: yes
Status: current

Change controller: IETF
Reference: RFC 9116

Field Name: Canonical
Description: canonical URI for this file
Multiple Appearances: yes
Status: current
Change controller: IETF
Reference: RFC 9116

Field Name: Contact
Description: contact information to use for reporting vulnerabilities
Multiple Appearances: yes
Status: current
Change controller: IETF
Reference: RFC 9116

Field Name: Expires
Description: date and time after which this file is considered stale
Multiple Appearances: no
Status: current
Change controller: IETF
Reference: RFC 9116

Field Name: Encryption
Description: link to a key to be used for encrypted communication
Multiple Appearances: yes
Status: current
Change controller: IETF
Reference: RFC 9116

Field Name: Hiring
Description: link to the vendor's security-related job positions
Multiple Appearances: yes
Status: current
Change controller: IETF
Reference: RFC 9116

Field Name: Policy
Description: link to security policy page
Multiple Appearances: yes
Status: current
Change controller: IETF

Reference: RFC 9116

Field Name: Preferred-Languages
Description: list of preferred languages for security reports
Multiple Appearances: no
Status: current
Change controller: IETF
Reference: RFC 9116

7. References

7.1. Normative References

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, DOI 10.17487/RFC2046, November 1996, <https://www.rfc-editor.org/info/rfc2046>.

[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>.

[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>.

[RFC2277] Alvestrand, H., "IETF Policy on Character Sets and Languages", BCP 18, RFC 2277, DOI 10.17487/RFC2277, January 1998, <https://www.rfc-editor.org/info/rfc2277>.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002, <https://www.rfc-editor.org/info/rfc3339>.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, DOI 10.17487/RFC3629, November 2003, <https://www.rfc-editor.org/info/rfc3629>.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, DOI 10.17487/RFC3966, December 2004, <https://www.rfc-editor.org/info/rfc3966>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005, <https://www.rfc-editor.org/info/rfc3986>.

[RFC4880] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, DOI 10.17487/RFC4880, November 2007, <https://www.rfc-editor.org/info/rfc4880>.

[RFC5198] Klensin, J. and M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, DOI 10.17487/RFC5198, March 2008, <https://www.rfc-editor.org/info/rfc5198>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", BCP 47, RFC 5646, DOI 10.17487/RFC5646, September 2009, <https://www.rfc-editor.org/info/rfc5646>.

[RFC6068] Duerst, M., Masinter, L., and J. Zawinski, "The 'mailto' URI Scheme", RFC 6068, DOI 10.17487/RFC6068, October 2010, <https://www.rfc-editor.org/info/rfc6068>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

[RFC7405] Kyzivat, P., "Case-Sensitive String Support in ABNF", RFC 7405, DOI 10.17487/RFC7405, December 2014, <https://www.rfc-editor.org/info/rfc7405>.

[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>.

[RFC8615] Nottingham, M., "Well-Known Uniform Resource Identifiers (URIs)", RFC 8615, DOI 10.17487/RFC8615, May 2019, <https://www.rfc-editor.org/info/rfc8615>.

7.2. Informative References

[CERT.CVD]

Software Engineering Institute, "The CERT Guide to Coordinated Vulnerability Disclosure", Carnegie Mellon University, CMU/SEI-2017-SR-022, August 2017.

[ISO.29147.2018] ISO, "Information technology - Security techniques - Vulnerability disclosure", ISO/IEC 29147:2018, October 2018.

[ISO.8601-1] ISO, "Date and time - Representations for information interchange - Part 1: Basic rules", ISO 8601-1:2019, February 2019.

[ISO.8601-2] ISO, "Date and time - Representations for information interchange - Part 2: Extensions", ISO 8601-2:2019, February 2019.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, DOI 10.17487/RFC2196, September 1997, <https://www.rfc-editor.org/info/rfc2196>.

[RFC2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", BCP 21, RFC 2350, DOI 10.17487/RFC2350, June 1998, <https://www.rfc-editor.org/info/rfc2350>.

[RFC3013] Killalea, T., "Recommended Internet Service Provider Security Services and Procedures", BCP 46, RFC 3013, DOI 10.17487/RFC3013, November 2000, <https://www.rfc-editor.org/info/rfc3013>.

[RFC7485] Zhou, L., Kong, N., Shen, S., Sheng, S., and A. Servin, "Inventory and Analysis of WHOIS Registration Objects", RFC 7485, DOI 10.17487/RFC7485, March 2015, <https://www.rfc-editor.org/info/rfc7485>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Acknowledgments

The authors would like to acknowledge the help provided during the development of this document by Tom Hudson, Jobert Abma, Gerben Janssen van Doorn, Austin Heap, Stephane Bortzmeyer, Max Smith, Eduardo Vela, and Krzysztof Kotowicz.

The authors would also like to acknowledge the feedback provided by multiple members of the IETF's LAST CALL, SAAG, and SECDISPATCH lists.

Yakov Shafranovich would like to also thank L.T.S. (for everything).

Authors' Addresses

Edwin Foudil
Email: contact@edoverflow.com

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