



XMPP

XEP-0268: Incident Reporting

Artur Hefczyc

<mailto:artur.hefczyc@gmail.com>

<xmpp:artur.hefczyc@tigase.org>

Florian Jensen

<mailto:admin@flosoft.biz>

<xmpp:admin@im.flosoft.biz>

Mickaël Rémond

<mailto:mickael.remond@process-one.net>

<xmpp:mremond@process-one.net>

Peter Saint-Andre

<mailto:stpeter@jabber.org>

<xmpp:stpeter@jabber.org>

<https://stpeter.im/>

Matthew Wild

<mailto:mwild1@gmail.com>

<xmpp:mwild1@jaim.at>

2009-11-17

Version 0.3

Status	Type	Short Name
Deferred	Standards Track	NOT_YET_ASSIGNED

This specification defines methods for incident reporting among XMPP server deployments.

Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 - 2011 by the [XMPP Standards Foundation](#) (XSF).

Permissions

Permission is hereby granted, free of charge, to any person obtaining a copy of this specification (the "Specification"), to make use of the Specification without restriction, including without limitation the rights to implement the Specification in a software program, deploy the Specification in a network service, and copy, modify, merge, publish, translate, distribute, sublicense, or sell copies of the Specification, and to permit persons to whom the Specification is furnished to do so, subject to the condition that the foregoing copyright notice and this permission notice shall be included in all copies or substantial portions of the Specification. Unless separate permission is granted, modified works that are redistributed shall not contain misleading information regarding the authors, title, number, or publisher of the Specification, and shall not claim endorsement of the modified works by the authors, any organization or project to which the authors belong, or the XMPP Standards Foundation.

Warranty

NOTE WELL: This Specification is provided on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE.

Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall the XMPP Standards Foundation or any author of this Specification be liable for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising from, out of, or in connection with the Specification or the implementation, deployment, or other use of the Specification (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if the XMPP Standards Foundation or such author has been advised of the possibility of such damages.

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF's Intellectual Property Rights Policy (a copy of which can be found at <http://xmpp.org/about-xmpp/xsf/xsf-ipr-policy/> or obtained by writing to XMPP Standards Foundation, 1899 Wynkoop Street, Suite 600, Denver, CO 80202 USA).

Contents

1	Introduction	1
2	Incident Reports	1
3	Incident Solutions	3
4	Processing of Incident Reports	4
5	Security Considerations	4
6	IANA Considerations	5
7	XMPP Registrar Considerations	5
	7.1 Protocol Namespaces	5
	7.2 Protocol Versioning	5
8	XML Schema	5

1 Introduction

As XMPP technologies have been deployed more widely, the open XMPP network has become a more significant target for attacks. This specification defines ways for XMPP server deployments to share information with each other and therefore to handle such attacks in a more real-time fashion. In particular, it defines a format for sharing incident reports among XMPP server deployments. (For some related considerations, see [RFC 2350](#)¹, [RFC 3067](#)², and [RFC 5070](#)³.)

2 Incident Reports

An incident report consists of an XMPP <message/> stanza containing an <incident/> child element that includes an 'id' attribute whose value is a UUID as described in [RFC 4122](#)⁴. An example is shown below. A server deployment SHOULD send incident reports only to peer servers that it trusts, for example peers that are in its "server roster" as described in [Server Rosters](#)⁵.

Listing 1: An incident report

```
<message from='jabber.org' to='im.flosoft.biz'>
  <incident xmlns='urn:xmpp:incident:0'
    id='BA51A035-7710-4558-9BBF-34838A4C5B24'>
    <description>
      <discuss>
        <admin>stpeter@jabber.org</admin>
        <muc>operators@conference.jabber.org</muc>
      </discuss>
      <info>
        <category>muc</category>
        <type>presence</type>
        <type>long-messages</type>
      </info>
      <locs>
        <loc>jdev@conference.jabber.org</loc>
        <loc>jabber@conference.jabber.org</loc>
      </locs>
      <rels>
        <rel>133BCE2E-E669-4ECE-B0F8-766B9E65630D</rel>
      </rels>
    </incident>
  </message>
```

¹RFC 2350: Expectations for Computer Security Incident Response <<http://tools.ietf.org/html/rfc2350>>.

²RFC 3067: TERENA's Incident Object Description and Exchange Format Requirements <<http://tools.ietf.org/html/rfc3067>>.

³RFC 5070: The Incident Object Description Exchange Format <<http://tools.ietf.org/html/rfc5070>>.

⁴RFC 4122: A Universally Unique Identifier (UUID) URN Namespace <<http://tools.ietf.org/html/rfc4122>>.

⁵XEP-0267: Server Rosters <<http://xmpp.org/extensions/xep-0267.html>>.

```
<severity>2</severity>
<source>
  <jids>
    <jid>abuser@abuse.lit</jid>
    <jid>loser@abuse.lit</jid>
  </jids>
</source>
<text xml:lang='en'>lots of MUC spammers from abuse.lit!</text>
<time>
  <begin>2009-04-13T19:05:20Z</begin>
  <end>2009-04-13T19:27:22Z</end>
  <report>2009-04-13T19:31:07Z</report>
</time>
</description>
</incident>
</message>
```

The defined children of the <description/> element are as follows:

Element Name	Description
<discuss/>	The JID of the server admin who generated the incident report (<admin/>), as well as a Multi-User Chat XEP-0045: Multi-User Chat <http://xmpp.org/extensions/xep-0045.html>. room where the incident can be discussed (<muc/>).
<info/>	Structured information about the incident. The defined values of the <category/> and <type/> elements shall be provided via a registry. It is envisioned that the <category/> values shall be "muc" for Multi-User Chat XEP-0045: Multi-User Chat <http://xmpp.org/extensions/xep-0045.html>. incidents, "pubsub" for Publish-Subscribe XEP-0060: Publish-Subscribe <http://xmpp.org/extensions/xep-0060.html>. incidents, "reg" for account registration (In-Band Registration XEP-0077: In-Band Registration <http://xmpp.org/extensions/xep-0077.html>.) incidents, and "stanzas" for general XMPP incidents.
<locs/>	The place or places on the XMPP network where the incident has occurred (such as a multi-user chat room, a publish-subscribe service, or a general XMPP server), each contained in a separate <loc/> element.
<rels/>	The IDs of one or more incidents to which this incident might be related, each contained in a separate <rel/> element.
<severity/>	The seriousness of the problem, from 5 (least serious) to 1 (most serious).
<source/>	The IPv4 or IPv6 address (optionally including port) and JabberID where the incident originated (multiple instance of each source type can be included).
<text/>	A natural-language description of the event. This element SHOULD possess an 'xml:lang' attribute. Multiple <text/> elements MAY be included, each with a different 'xml:lang' value.
<time/>	The time when the incident began and ended (include an empty <end/> element if the incident is still happening) and, optionally, was reported. The dates MUST conform to the DateTime profile specified in XMPP Date and Time Profiles XEP-0082: XMPP Date and Time Profiles <http://xmpp.org/extensions/xep-0082.html>.

3 Incident Solutions

If the reporting entity determines a solution to the problem or a receiving entity has a suggested solution to the problem, it SHOULD send out a revised incident report containing a <solution/> element (alternatively, the reporting entity can include a solution in its initial report). The solution element can include any of the elements defined for the <description/> element, such as the <ip/> element (since the XMPP server of a source JID might know the IP address and port of the connected entity).

Listing 2: An incident solution

```
<message from='jabber.org' to='im.flosoft.biz'>
  <incident xmlns='urn:xmpp:incident:0'
    id='BA51A035-7710-4558-9BBF-34838A4C5B24'>
    <description>
      ...
    </description>
    <solution>
      <source>
        <ips>
          <ip>192.0.2.1:53667</ip>
        </ips>
      </source>
      <text xml:lang='en'>iptables -A INPUT -s 192.0.2.1 -j DROP</text
    >
    </solution>
  </incident>
</message>
```

4 Processing of Incident Reports

Unless explicitly configured to do so, a receiving server SHOULD NOT automatically modify its configuration based on receipt of an incident report, even from a trusted server, but instead SHOULD prompt the human administrators so that they can take appropriate action.

A receiving server MAY accept incident reports from peers that are not on its "trust list", but SHOULD treat such reports with caution and provide them to the human administrator(s) of the server.

A receiving server MAY forward reports that it receives to other servers it trusts.

5 Security Considerations

This technology is designed to help mitigate attacks on the XMPP network. However, incident reporting is itself vulnerable to the following attacks:

- False reports could lead a server to deny service to legitimate users or peer servers (see also [Best Practices to Discourage Denial of Service Attacks](#)⁶). To help mitigate such attacks, a server SHOULD treat with caution any incident reports that it might receive from untrusted entities.
- If traffic between two servers is not protected using Transport Layer Security (TLS), a passive eavesdropper could gain access to incident reports and therefore adjust its behavior in response. To prevent such attacks, servers SHOULD use TLS.

⁶XEP-0205: Best Practices to Discourage Denial of Service Attacks <<http://xmpp.org/extensions/xep-0205.html>>.

6 IANA Considerations

This document requires no interaction with the [Internet Assigned Numbers Authority \(IANA\)](#)⁷.

7 XMPP Registrar Considerations

7.1 Protocol Namespaces

This specification defines the following XML namespace:

- urn:xmpp:incident:0

Upon advancement of this specification from a status of Experimental to a status of Draft, the [XMPP Registrar](#)⁸ shall add the foregoing namespace to the registry located at <http://xmpp.org/registrar/namespaces.html>, as described in Section 4 of [XMPP Registrar Function](#)⁹.

7.2 Protocol Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

8 XML Schema

```
<?xml version='1.0' encoding='UTF-8'?>

<xs:schema
  xmlns:xs='http://www.w3.org/2001/XMLSchema'
  targetNamespace='urn:xmpp:incident:0'
  xmlns='urn:xmpp:incident:0'
  elementFormDefault='qualified'>

  <xs:element name='incident'>
```

⁷The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <http://www.iana.org/>.

⁸The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <http://xmpp.org/registrar/>.

⁹XEP-0053: XMPP Registrar Function <http://xmpp.org/extensions/xep-0053.html>.

```
</xs:element>

<xs:simpleType name='empty'>
  <xs:restriction base='xs:string'>
    <xs:enumeration value=''/>
  </xs:restriction>
</xs:simpleType>

</xs:schema>
```