Prosody XMPP server advisory 2022-01-13 (Remote Denial of Service)

Prosody XMPP server advisory 2022-01-13 (Remote Denial of Service)

Project
    Prosody XMPP server
URL
    https://prosody.im/
Date
    2022-01-13

References

- Advisory (HTML): https://prosody.im/security/advisory_20220113/
- Advisory (text): https://prosody.im/security/advisory_20220113.txt
- Link to patch: https://prosody.im/security/advisory_20220113/1.patch
- Instructions for testing a deployment (will only be published a few days after this announcement): https://prosody.im/security/advisory_20220113/instructions.txt

This advisory details a new security vulnerability discovered in the Prosody.im XMPP server software. A fix for this issue is available in Prosody 0.11.12, we advise everyone affected to upgrade.

Unauthenticated Remote Denial of Service Attack in the WebSocket interface

CVE
    CVE-2022-0217
CVSS

7.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:X/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:H)

CWEs
: CWE-776, CWE-20, possibly CWE-611

Affected versions
: All versions with support for WebSockets

Fixed versions
: 0.11.12

Description

It was discovered that an internal Prosody library to load XML based on libexpat does not properly restrict the XML features allowed in parsed XML data. Given suitable attacker input, this results in expansion of recursive entity references from DTDs (CWE-776). In addition, depending on the libexpat version used, it may also allow injections using XML External Entity References (CWE-611). The Prosody team did not evaluate if and which versions are affected by external entity reference expansion.

The internal prosody API was meant for local access of trusted XML data, but has since started to be used for network-facing applications. An audit of usages of this API in prosody code revealed that it is used by the WebSockets module, which allows to use XMPP over WebSockets.

As the WebSockets module needs to parse XML in order to start a session before authentication, the lack of restriction of available XML features can be used in a Billion Laughs Attack in order to cause excessive resource consumption and denial of service. Because Prosody does not yield control to other connections while processing a fully received WebSocket frame, this also results in Denial of Service.

This internal API is *not* used to handle XML on normal XMPP connections or the BOSH interface, which are hence not affected by this vulnerability.

Affected configurations

All Prosody servers with WebSockets enabled and the WebSockets endpoint exposed directly to any untrusted party are affected.

Mitigating factors

WebSockets are not enabled by default.

Workaround

The recommended mitigation is to upgrade to Prosody 0.11.12, released on 2022-01-13. Follow the manual patching instructions only if you cannot immediately upgrade.

This advisory has a patch attached, it can be applied to any Prosody installation from the 0.11 series. The patch is already applied in 0.11.12. If the patch is applied manually and your Prosody installation is managed by a package manager (such as apt or dnf), a future update will revert the change.

To do so, open a normal shell on the server and locate the file xml.lua. It should exist in a directory structure `util/xml.lua`.

On Debian, it is found in

```
/usr/lib/prosody/util/xml.lua
```

on 0.11.x or

```
/usr/share/lua/5.1/prosody/util/xml.lua
```

on trunk

Navigate to the directory containing the `xml.lua` file and apply the attached patch using `patch -p2 < 1.patch`.

- Link to patch: https://prosody.im/security/advisory_20220113/1.patch

Now restart Prosody. There is no known-to-be-safe way to reload the util/xml.lua file without a complete Prosody restart.

After the restart, this vulnerability is fixed.

If neither patching nor upgrading is an option, it is possible to unload the websocket module on Prosody trunk using:

```
prosodyctl shell module unload websocket
```

On 0.11.x and earlier, you need to

- use `module:unload("websocket")` from the telnet console, OR
- unload the module via an XMPP Ad-Hoc command OR

- if neither of these online ways are available, remove the module from the configuration and restart prosody.

However, note well that third-party modules may also use the vulnerable internal APIs to parse XML. Unloading websocket does not protect those other modules; only the patch or the upgrade can do that.

Fix

This issue is fixed in Prosody 0.11.12 by restricting the available XML features in the internal XML API.

Attribution

The issue was discovered during internal code review by Matthew Wild during the development of another feature. The patch was developed by Jonas Schäfer. A proof-of-concept exploit was developed by Jonas Schäfer and Kim Alvefur and will be published soon to allow administrators to check their instances.

Timeline

2022-01-10: Discovery of the issue, development of an exploit as well as an initial patch. Sharing of this information with Jitsi and Snikket developers. Heads-up sent to the Snikket group chat.

2022-01-11: Refinement of the patch, release preparation. Heads-up sent to the Prosody group chat. Patch shared confidentially with Jitsi.

2022-01-12: Continued release preparation, notification of distros@.

2022-01-13: Coordinated Snikket and Prosody release with a fix, publication of the advisory.