About Deskpro On-Premise and the Log4j 0-day vulnerability

2021-12-13 - Christopher Nadeau - Comments (0) - News

On 9th December, a high severity vulnerability in a popular software library Log4j was disclosed publicly (CVE-2021-44228). This library is used in thousands of projects across every industry, and so this particular vulnerability has garnered a lot of attention as organisations hurry to implement mitigations and fixes.

Deskpro itself does not use this library, so Deskpro itself is unaffected. However, Deskpro uses Elasticsearch, a search server published by Elastic, which *does* use this library. Elastic posted a security announcement on 10th December outlining the impact of this vulnerability with their software.

Note
Note that Elastic have made several amendments to their announcement as late 14th December, so if you already have read the post, we recommend reading it again in case the advice relevant to your situation has changed.

Urgency
You should consider this vulnerability extremely urgent. It could allow Remote Code Execute (RCE) which could lead to your services being completely compromised.

Summary
Deskpro and your use of Elasticsearch with Deskpro may be affected depending on several factors outlined below.

- □ Deskpro Cloud customers: Our Cloud infrastructure was unaffected. We've deployed updates anyway as a precaution.
- Deskpro On-Premise customers using Deskpro 5.x, 2019.x, 2020.x, 2021.1.x, 2021.2.x.
    - □ When using the VM image or automated installer scripts: You are unaffected. These versions of Deskpro shipped with Elasticsearch 2.x which is unaffected.
    - ⚠ If you use Deskpro with an external or manually configured Elasticsearch host, or if you have manually configured or updated Elasticsearch on your

server, then you need to ask your sysadmin or service provider to check if you are vulnerable. If vulnerable, you will need to follow the advice listed in Elastic's security announcement.

    - ⚠ Windows and Windows Installer: You should follow these instructions to address the issue, which include upgraded to Elasticsearch 5.6.16 and applying the `-Dlog4j2.formatMsgNoLookups=true` flag per guidance here.

- If you are using Deskpro On-Premise Controller with Deskpro Horizon (>= 2021.40, our major new update from about a month ago)
    - □ When using the default Elasticsearch service that ships with the product, then your instance is not vulnerable. Elastic has promised to release updates as a precautionary measure anyway - and we'll release an update to Deskpro On-Premise as soon as that is available.
    - ⚠ If you are using Deskpro On-Premise with Deskpro Horizon but have chosen to use an external Elasticsearch service, then your external service may be vulnerable. You need to ask your sysadmin or service provider to check. If vulnerable, you will need to follow the advice listed in Elastic's security announcement.

Your next actions

Generally speaking, if you are using Elasticsearch >=5.x (which is everyone *except* for customers using the default Elasticsearch 2.x provided with the VM image and installer scripts), then you should update your Elasticsearch server with the updates Elastic has published. Even if your version of Elasticsearch is not specifically mentioned as being vulnerable, you should update anyway as a precaution.

And in all cases - we recommend taking the opportunity to look closely at your infrastructure to make sure there are no other vulnerable components in your stack. For example, Elastic publishes many other tools such as Logstash which are affected in other ways, and of course you may be using other vulnerable software that is unrelated to Deskpro.