Log4Shell vulnerability in panagenda products - CVE-2021-44228, CVE-2021-4104, CVE-2021-45046

What has happened?

Recently a critical vulnerability (CVE-2021-44228) was discovered in the Apache Log4j library. This vulnerability can be exploited remotely without authentication and allows remote code execution. It ranks a 10 out of 10 on the CVSS severity level. It has pretty much set the world aflame. You can get more about what happened here and an overview with more links here.

More vulnerabilities are being discovered (CVE-2021-4104, CVE-2021-45046), information on them can be found below.

Are panagenda products affected?

Yes. CVE-2021-44228 affects several of our products.

Update 2021-12-14: Another vulnerability related to Log4j has popped up: CVE-2021-4104. None of our products are vulnerable to this new CVE.
Update 2021-12-15: **A third vulnerability, CVE-2021-45046, has been discovered. Some of our products are vulnerable.** This CVE is only classed as a 3.7 out of 10, and can only be used to perform a DOS (denial-of-service) attack.
Update 2021-12-17: The above CVE-2021-45046 now had its severity level increased to 9, and also allows remote code execution. Still, Metabase says they are not using non default configurations, which makes it not vulnerable.
Update 2021-12-19: Another Log4j exploit has been reported: CVE-2021-45105. Apache classes it as a 7.5, it can be used to execute a DOS attack.

After the first vulnerability was published, we immediately started checking all our products for exposure to it. **As was to be feared, many of our products use Log4j (or include third-party components that do), are therefore vulnerable, and need to be updated.**

- ApplicationInsights, ConnectionsExpert, iDNA, and iDNA Applications use some Log4j directly. Starting with the versions shown in the column "Fix Release [1]" we will remove Log4j completely to resolve this and reliably prevent any further issues.
- GreenLight, iDNA Applications, and OfficeExpert include Metabase which uses Log4j. We will update the Metabase version in all these products to a safe release.

Overview and Status

Product	CVE-2021-44228	Fix Status	Fix Release [1]		CVE-2021-45046 / CVE-2021-45105	Fix Status	Fix Release [2]		How To Upgrade
ApplicationInsights	vulnerable - fix available	released	1.6.3		vulnerable - fix available	released	1.6.3		Upgrade ApplicationInsights (v1.5.1)
ConnectionsExpert 2.x	vulnerable - fix available	released	2.1.3		vulnerable - fix available	released	2.1.3		Upgrade ConnectionsExpert (> v2.0)
ConnectionsExpert 3.x	vulnerable - fix available	released	3.1.3		vulnerable - fix available	released	3.1.3		Upgrade ConnectionsExpert (> v2.0)
GreenLight	vulnerable - fix available	released	4.5.0		vulnerable - fix available	released	4.5.1		Upgrading GreenLight - only for >=3.5.x
iDNA	vulnerable - fix available	released	2.11.1		vulnerable - fix available	released	2.11.1		Please contact support - all customers should be migrated to iDNA Applications already.
iDNA Applications	vulnerable - fix available	released	2.1.2		vulnerable - fix available	released	2.2.1		Upgrading iDNA Applications
MarvelClient	safe				safe				
OfficeExpert	vulnerable - fix available	released	4.3.3		vulnerable - fix available	released	4.3.3		Upgrading OfficeExpert
					Metabase vulnerable [3]	waiting for Metabase	4.3.4		
OfficeExpert EPM	safe				safe				
SecurityInsider / GroupExplorer	safe				safe				
SmartChanger	safe				safe				
Document Properties Plugin	safe				safe				
LogViewer Plugin	safe				safe				
Network Monitor Plugin	safe				safe				
PrefTree Plugin	safe				safe				
Tabzilla Plugin	safe				safe				

Timezone Helper Plugin	safe				safe				

1) The fix releases in this column address CVE-2021-44228 both in our own code, and in Metabase.
2) The fix releases in this column address CVE-2021-45046 and CVE-2021-45105. In some cases there are separate rows for cases where the older fix solves the issue in our code, but a newer fix with an updated Metabase version is needed to fix it there. See also 3).
3) To mitigate any remaining risk until we release a version with the updated Metabase release, see info box "Regarding Metabase" below.

Regarding Metabase

Metabase includes Log4j and is vulnerable to CVE-2021-44228. For a first fix we update to Metabase 0.40.7 (which includes Log4j 2.15.0 and protects from the remote code execution exploit). Releases with this fix can be found in the left part of the table above. (column marked with [1])

The more recently discovered CVE-2021-45046 requires Log4j 2.16.0, and the even more recent CVE-2021-45105 requires 2.17.0. Both CVEs are fixed in our own code (release in column marked with [1]), but we are waiting for the Metabase release which includes 2.17.0 for our next release.
Until then, you can go with the release that fixes the problem in our code and manually turn off Metabase:

- Connect to the appliance with ssh or putty
- For GreenLight:

```
docker stop gl_metabase
```

- For OfficeExpert and iDNA Applications:

```
docker stop panagenda_metabase
```

What happens now? What do I need to do?

You will need to update any products that are affected. The releases in the left part of the table (column marked with [1]) are the important update to protect you against the more severe CVE and should be applied ASAP. The last release to fix less severe issues in Metabase is in the works.

Our service and support teams are contacting all our customers to answer questions and help where needed. Please send requests and questions to support@panagenda.com

We will keep updating this post with more information as it becomes available.