hubbl™
DIAGNOSTICS

AUTHOR: MIKE BOGAN

Director of Product Strategy

Out-of-date installed package risks: How many are in your Salesforce org?

Is your Salesforce org at risk from out-of-date installed packages? Were you even aware that out-of-date installed packages could be putting your org at a greater security risk?

> **It's crucial to understand the potential risks associated with not updating your installed packages.**

In the age of workflow and process retirement, out-of-date packages may be slowing down your org with legacy declarative automation. You also run the risk of potential security vulnerabilities stemming from custom code in out-of-date packages. Additionally, there's a chance installed packages haven't gone through the AppExchange Security Review process (privately listed applications) creating even more vulnerabilities.

Unfortunately, Salesforce has never made this a simple thing for Salesforce teams to manage. Even if you check for new package versions manually (a time consuming task), there's no guarantee you'll find them or that publishers update the correct AppExchange version.

In fact, according to the 2023 Benchmark Report on Salesforce Optimization, on average:

- 99% of orgs have installed packages with newer versions available.
- Salesforce orgs have 14 installed packages with newer versions available.
- 8% of these packages are both out-of-date and haven't undergone security review.

DOWNLOAD: 7 CRITICAL ORG OPTIMIZATIONS INSIGHTS FOR HIGH-PERFORMING SALESFORCE TEAMS

Clearly, we have a big challenge in the ecosystem! So let's tackle what you need to know to manage them effectively... and how to do it quickly.

What are installed packages?

The Salesforce AppExchange launched in 2006, two years before the Apple App Store. According to Salesforce, it's grown to over 7000 apps with over 10 million installs and 91% of Salesforce customers have installed at least one AppExchange app.

Salesforce AppExchange apps are installed packages that are distributed as managed or unmanaged:

- **Managed packages** are maintained by the publisher and can be upgraded
- **Unmanaged packages** have code that can be seen and modified but not upgraded

However, Salesforce AppExchange apps are not the only type of installed package. Installed packages can be created by any developer with access to a Salesforce org. This means packages could be installed from a third party, like a consultant or developer working in your org.

Are your installed packages security reviewed?

Salesforce states that "private listings do not go through a security review and administrators should inspect the application carefully before determining whether it should be installed within their organization." Salesforce offers support by showing you whether an installed package has undergone security review in the Setup > Installed Packages page.

It's definitely worth checking out—not only have these apps not undergone security review, but if there's an upgrade you won't know unless the publisher reaches out to you.

How to keep your installed packages up-to-date?

So what happens when a publisher upgrades a package that's on the AppExchange? If it's managed, often the publisher will push the upgrade to your org and you get the latest version. Sometimes you have to initiate the package upgrade yourself. In those scenarios, you need to know there's a newer version available. If you miss an announcement or there is none, you're out of luck.

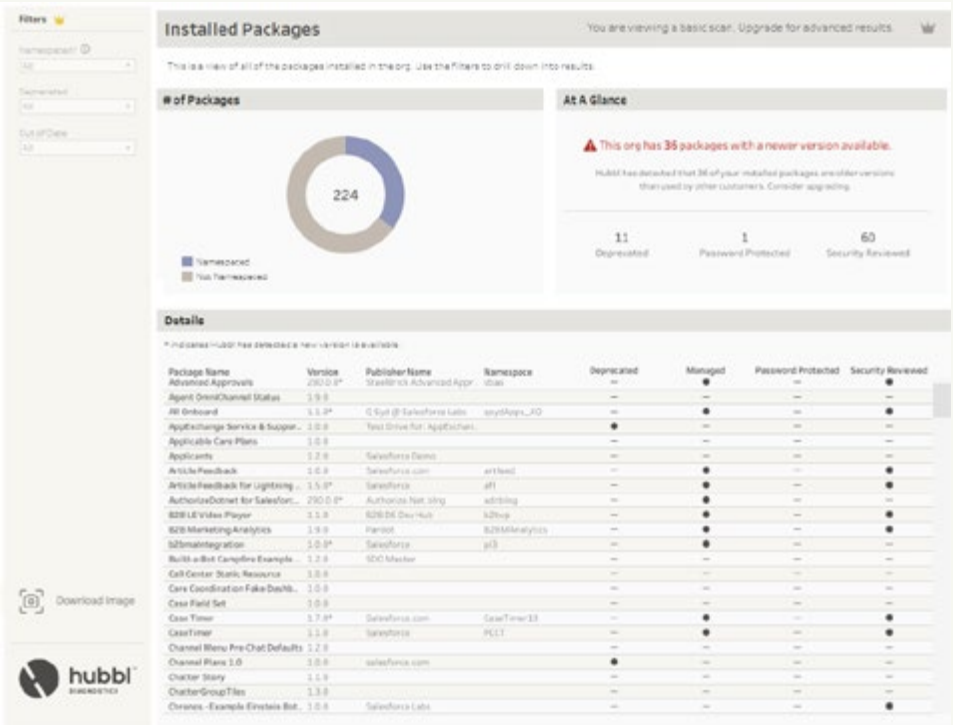
Even if you went through the time-consuming manual process of checking for yourself (by going into Setup > Installed Packages, checking the version number, and comparing to the AppExchange), there's no guarantee the publisher even updated the AppExchange version number, as they have to do that manually. To put it simply, even if you checked the AppExchange, there still may be a newer version available.

This is why it's incredibly important to have regular updates to installed packages and audits to minimize all risks and ensure compliance. With all the businesses and work Salesforce admins are faced with day in and day out, it's about time we had a solution to gain control over these issues and mitigate these security risks.

> **There needs to be a better way to help admins identify whether newer versions of public and privately listed installed packages are available.**

There is a better way, and yes, it's automated!

Organizations are now able to gain insight on installed packages, ensuring they meet specific security and compliance requirements—and it's free.



hubbl™
DIAGNOSTICS

Hubbl Diagnostics Essentials provides a custom code security review that can be used to review custom code that is unpackaged or in unlocked unmanaged packages. By analyzing the configurations and usage patterns, the tool can identify potential compliance gaps and recommend specific actions to address them—meeting your security requirements.

For package versioning, Hubbl Diagnostic's unique aggregate view of the Salesforce ecosystem allows us to check all your installed packages, either privately listed or from the AppExchange, against our database of package versions installed in other orgs. This "crowd-sourced" data set ensures that you'll have a better chance of keeping your org up-to-date with the latest features, reduce security risks and speed up your org by removing legacy declarative automation like workflow and processes.

So, how many out-of-date packages are in your org?

Find your out-of-date installed packages for free

Hubbl Diagnostics Essentials identifies installed packages with newer versions available, provides a custom code security review, and more.

TRY IT FREE