GOhack24

Atlassian under the Hood
Vulnerability & Malicious Plugin Research

Manuel Kiesel, cyllective AG
mkiesel.ch↗ / @rtfmkiesel↗

📋 to-do list for today

- the Atlassian ecosystem
- malicious plugin capabilities & live demo
- plugin vulnerability research
- q&a

products

You know and probably use them:

- Confluence → wiki
- Jira → ~~hell~~ issue & project tracking
- Bitbucket → git
- ...

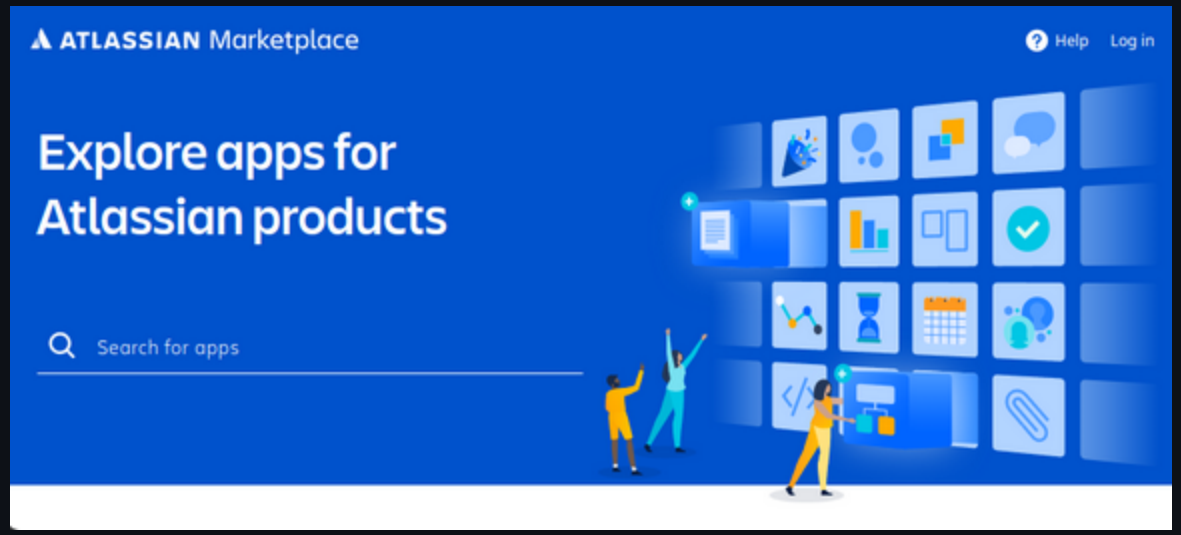
Today, we're gonna focus mainly on Confluence with a little bit of Jira.

products under the hood

- Mostly Java 8
- Served via Apache Tomcat
- Connects to a database (Oracle, MySQL, PostgreSQL, Microsoft SQL Server)

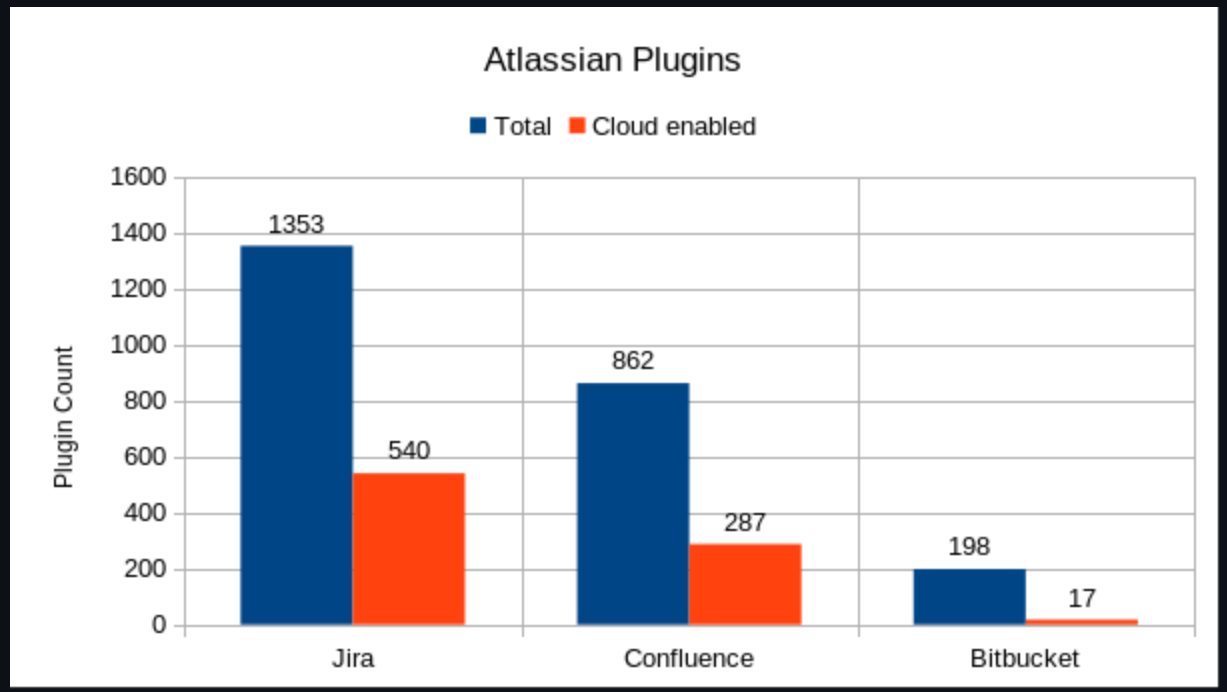
the marketplace

The Atlassian Marketplace↗ is the "app store" for Atlassian products.



the marketplace

Some stats about plugins, scraped on 30.09.2024:



the marketplace

Atlassian does not actively delist inactive or outdated apps.

Fun Fact: a handful of plugins are registered via an email whose domain you can buy today --> something something supply chain attack

the marketplace

To get listed in the marketplace, you need to meet some requirements↗

There is a "review process"↗ of your code:

> Security: Security checks and vulnerabilities scans completed to reduce risk and critical issues for customers.

the marketplace

What exactly happens during the review is not publicly documented.

Questions:

- What exactly is checked?
- Manual analysis or SAST?
  - > … our team … Scans and validates security results
- Is this only on the first listing?
  - What about (malicious) updates?

plugin capabilities

What can a plugin do?

Based on the modules you use, you can:

- REST module → Add REST API endpoints to the instance
- Servlet module → Use Java servlets
- Macro module → Use a form of HTML templates
- Web resource → Push JavaScript onto clients

However you can write any Java 8 compliant code.

malicious plugin live demo

malicious plugin capabilities

- No restrictions when accessing
  - any user
  - any data (wiki, issues & co.)
  - the underlying server (filesystem, commands)
  - the connected database

github.com/cyllective/malfluence↗

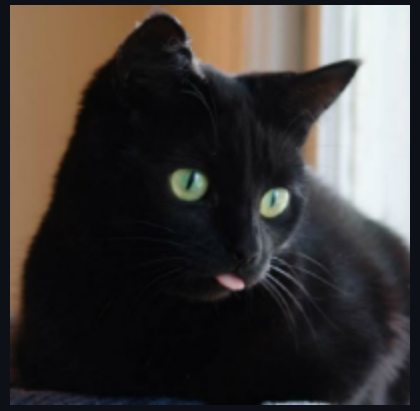
malicious plugin infection

How do you get a malicious plugin into your system?

- You manually install a (shady) plugin.
- You get hit by a supply chain attack on existing, already installed plugins.
- Your admin gets hit by an XSS.

vulnerability research

by cyllective's



@_cydave↗

plugin vulnerabilities

Since the core of Confluence & Jira is web, you have classic web vulns:

- Cross-Site-Scripting (XSS)
- SQL injection
- XML external entity (XXE) injection
- Insecure deserilization (of Java objects)
- Command Injection

xss payloads

- Make yourself admin (target = admin)
- Get RCE on the server by installing a plugin (target = admin)
- Takeover some ones account using a personal access token (target = anyone)

github.com/cyllective/XSS-Payloads/tree/main/Confluence↗

why does this work

- CSRF check can be disabled using `X-Atlassian-Token: no-check`
- Atlassian does not offer a CSP guideline ¯\(ツ)/¯
- `websudo` is potentially useless (was not able to verify)
  - … REST and XML-RPC APIs are not affected by secure administration sessions.

finding vulns

finding vulns

1. Scrape all data center plugins from the marketplace
2. Decompile `.jar` or `.obr` files using jadx↗
3. ???
4. Profit!

results

- 👾 53 0-days 👾
- Vulnerabilities
  - XSS
  - SQL Injection
- Products
  - 14x Jira
  - 39x Confluence

disclosure process

Atlassian: How to not handle a coordinated vulnerability disclosure

- Only selected plugins in bug bounty program (only cloud versions)
- No direct contact @Atlassian for plugin security issues
- Options:
  - Contact Atlassian with all vulns → did not work
  - Contact all plugin authors individually → ¯\(ツ)/¯
- After blog post → Atlassian finally responded

conclusion


ATLASSIAN
EVERYTHING
EVERYWHERE
ALL AT ONCE

conclusion

Plugins can do everything everywhere all at once on your system

To protect yourself:

- Install as little plugins as possible & audit your plugins.
- Monitor plugin updates against supply chain attacks.
- Do not use admins for daily use. (Admin XSS = RCE)

questions?

the end

Thank you for listening, and thanks to GObugfree for having me!

links

- cyllective: Auditing Atlassian Plugins, 53 0-Days Later↗
- cyllective: Creating a Malicious Atlassian Plugin↗

contact

- hi@mkiesel.ch↗
- mkiesel.ch↗ / @rtfmkiesel↗