

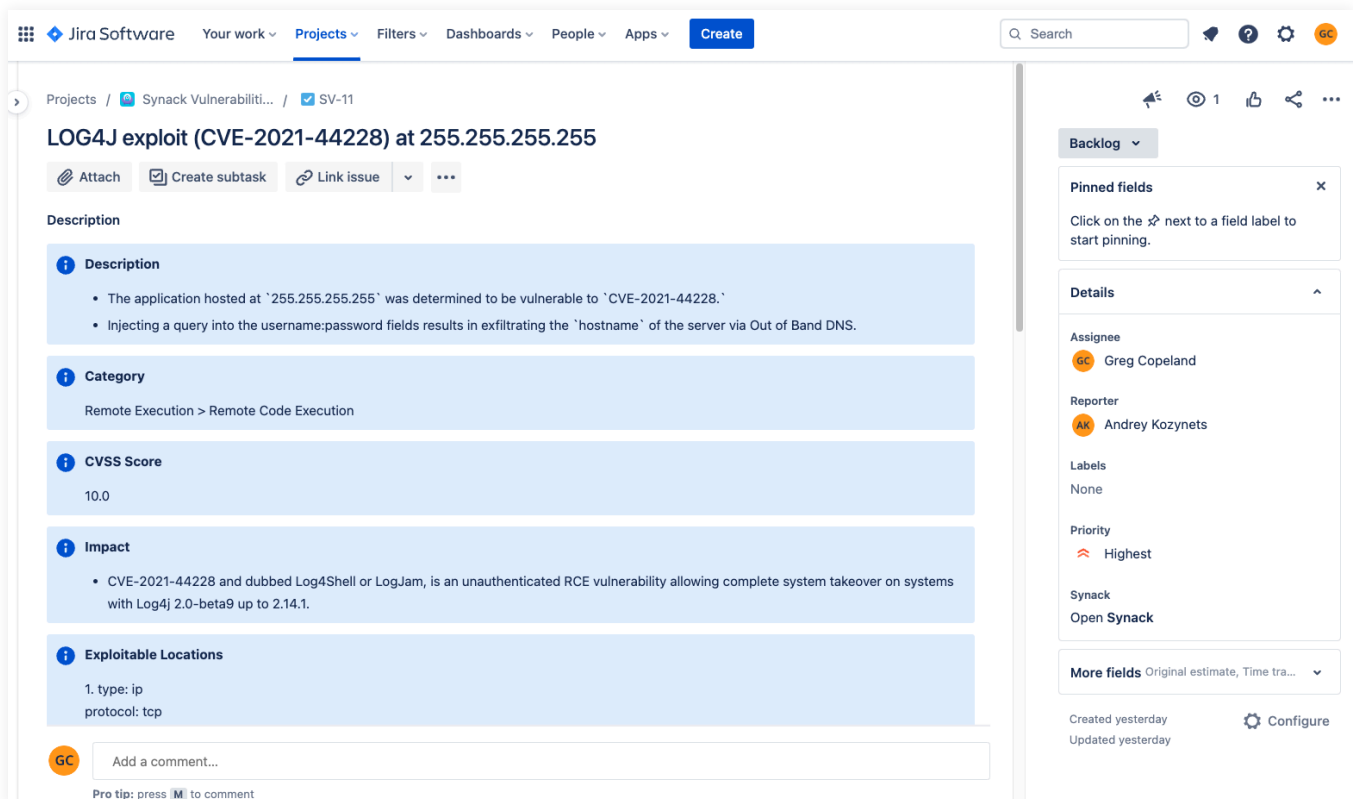
Jira and Synack

Integrating Security Testing with SDLC Workflows

Easy, continuous security validation with Synack & Jira

If you want a continuous and agile development lifecycle, while reducing the risk of being undermined by introducing a lot of vulnerabilities, you need to merge your cybersecurity and development workflows. The Synack App for Jira integrates Synack vulnerability findings with your existing Software Development Life Cycle (SDLC) workflows to help you remediate vulnerabilities more effectively and efficiently. By integrating Synack and Jira instances, we've removed the inefficiencies that come with vulnerability management and development being independent, unintegrated workflows.

This integration not only helps your engineering team remediate vulnerabilities quickly, its patch verification also helps ensure that the same vulnerabilities aren't being re-introduced in future code deployment. Anytime you make an update on Synack's platform or Jira, the change will be synced to both platforms. With this bi-directional capability, you can easily take the vulnerability data and status from your Synack security tests and make it more actionable and manageable for your team.



The screenshot displays a Jira ticket interface for a Synack vulnerability. The ticket title is "LOG4J exploit (CVE-2021-44228) at 255.255.255.255". The description is structured as follows:

- Description:**
 - The application hosted at `255.255.255.255` was determined to be vulnerable to `CVE-2021-44228`.
 - Injecting a query into the username:password fields results in exfiltrating the `hostname` of the server via Out of Band DNS.
- Category:** Remote Execution > Remote Code Execution
- CVSS Score:** 10.0
- Impact:**
 - CVE-2021-44228 and dubbed Log4Shell or LogJam, is an unauthenticated RCE vulnerability allowing complete system takeover on systems with Log4j 2.0-beta9 up to 2.14.1.
- Exploitable Locations:**
 - type: ip
 - protocol: tcp

The right sidebar shows the following fields:

- Assignee:** Greg Copeland
- Reporter:** Andrey Kozynets
- Labels:** None
- Priority:** Highest
- Synack:** Open Synack
- More fields:** Original estimate, Time tra...
- Created:** yesterday
- Updated:** yesterday

Sample Synack data in Jira ticket

Why integrate Synack and Jira?

Synack offers insights and intelligence by delivering reports of exploitable vulnerabilities discovered through our premier security testing platform that seamlessly integrates the adversarial perspective of the world's best security researchers, the Synack Red Team (SRT), with our continuous scanning technology. When you integrate your Jira Projects with Synack data, you can increase engineering team collaboration and communication to seamlessly find and remediate vulnerabilities, shifting your SDLC workflows to a cadence that enables continuous but secure delivery. A Jira ticket with vulnerability data from Synack not only alerts your engineering team, it provides real-time updates on researcher communication and vulnerability status updates to make sure you always have security information at your fingertips.

Benefits of the Jira-Synack bi-directional integration include:

- **Task Delegation:** Automatically create tickets within Jira when new vulnerabilities are surfaced by the Synack Platform.
- **Workflow Automation:** Manage the entire lifecycle of these incidents within Jira. Eliminate the duplicative process of updating vulnerability information in Jira instances and the Synack Platform.
- **Team Communication & Collaboration:** Keep comments and tags in sync between Jira Projects and Synack Assessment.
- **Fast & Efficient Remediation:** Streamline remediation through assigning vulnerabilities to specific stakeholders and requesting patch verification by Synack directly from Jira.

How it works

Any time new vulnerabilities are reported by the Synack Platform, these reports will be populated within your Jira Project automatically based on the predefined configurations and field mappings.

A number of configurations are available and allow you to map statuses and fields. Anytime you make an update on the Synack Platform or on Jira, the change will be synced to both platforms, allowing you to see the same information everywhere.

SYNACK FIELDS AVAILABLE IN JIRA INSTANCE WITH DOWNSTREAM & UPSTREAM INTEGRATION

Vulnerabilities	Every time a researcher submits a vulnerability on the Synack Platform, a new Jira ticket is created.
Researcher messages	If a researcher has a comment, he/she can update it on the Synack Platform, and it will appear in Jira.
Status change	If or when the status of a vulnerability (ticket, priority, assignee) changes in Jira, it will update on the Synack Platform too.
Multiple Jira instances	It is possible to map vulnerabilities to multiple Jira projects.

Getting started with Synack's Jira integration

You can access Synack's App for Jira in a free, simple, and easy way. It's a plug-and-play App that seamlessly installs on your existing Jira subscription and can be configured to work with your Synack Platform subscription within a matter of minutes. The Synack App for Jira is supported for on-premise (server and data center) and cloud instances of Jira.

The marketplace link is here:

<https://marketplace.atlassian.com/apps/1220818/synack-app-for-jira>

Contact your Synack program manager, or our tech alliance team for further information technologypartners@synack.com