

## ASM JIRA INTEGRATION

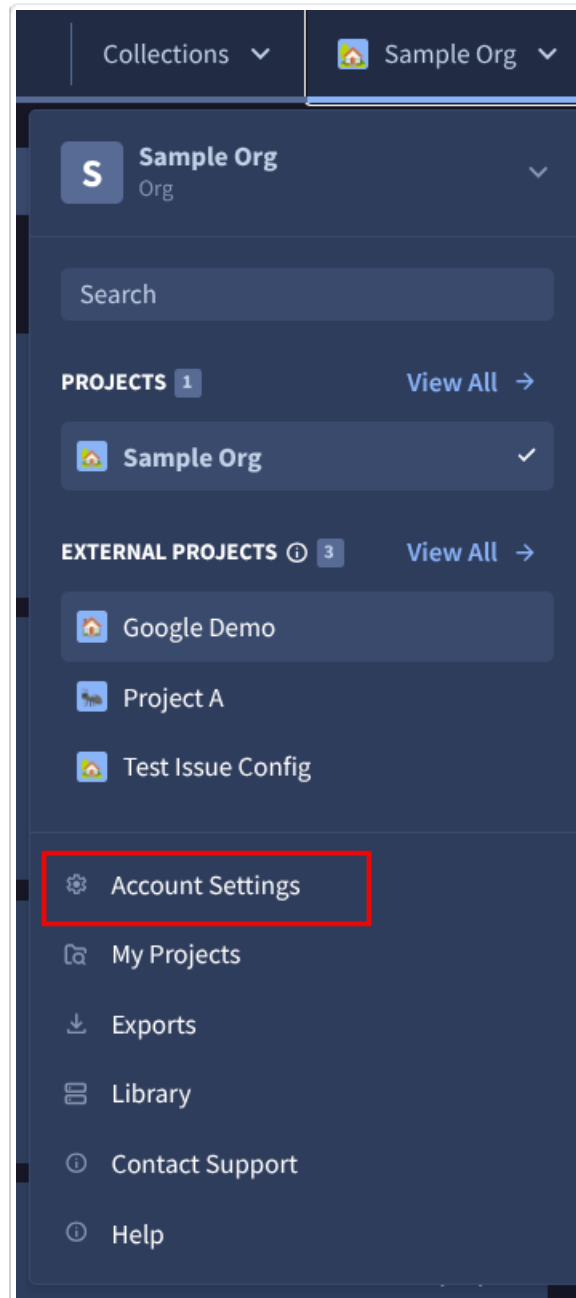


This integration is only available for Jira Cloud. Jira Data Center (on-prem) is not supported.

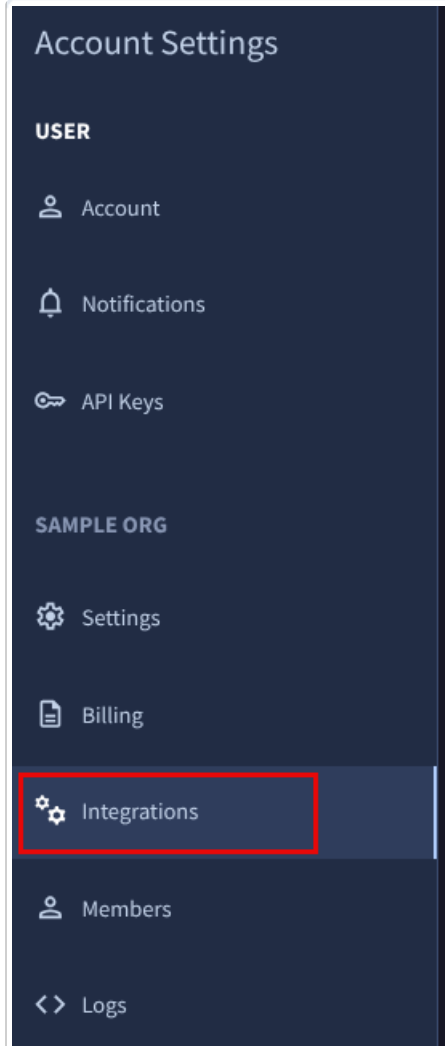
Jira is a powerful work management tool for all kinds of use cases. While using Mandiant Advantage Attack Surface Management (MA-ASM), you can use Jira for the purpose of Issue tracking and management. After you integrate Jira into MA-ASM, you can create Jira tickets directly from Issues in MA-ASM. No copy and paste is necessary; Issue details are pre-populated in the Jira ticket.

### Configure Jira integration

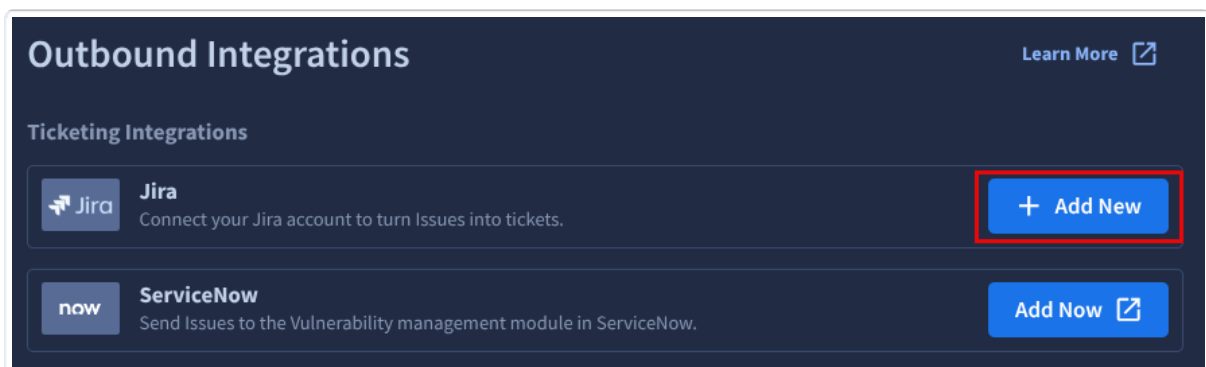
1. From the **Projects and Settings** menu in MA-ASM, select the appropriate Project, and then click **Account Settings**.



2. Click the **Integrations** tab.



3. In **Outbound Integrations**, click **Add New** for **Jira**.



4. On the **Connect your Jira Account** screen, enter your **Email**, **Host**, and **Jira API Key**.

 For more information, see [Manage API tokens for your Atlassian account](https://support.atlassian.com/atlassian-account/docs/manage-api-tokens-for-your-atlassian-account/) (<https://support.atlassian.com/atlassian-account/docs/manage-api-tokens-for-your-atlassian-account/>).

## Connect your Jira Account

**Jira Integration**

Navigate to your [Jira Cloud Account](#) to generate an API token. [Learn more here.](#)

**Email**

**Host**

**Jira API Key**

**Connect**

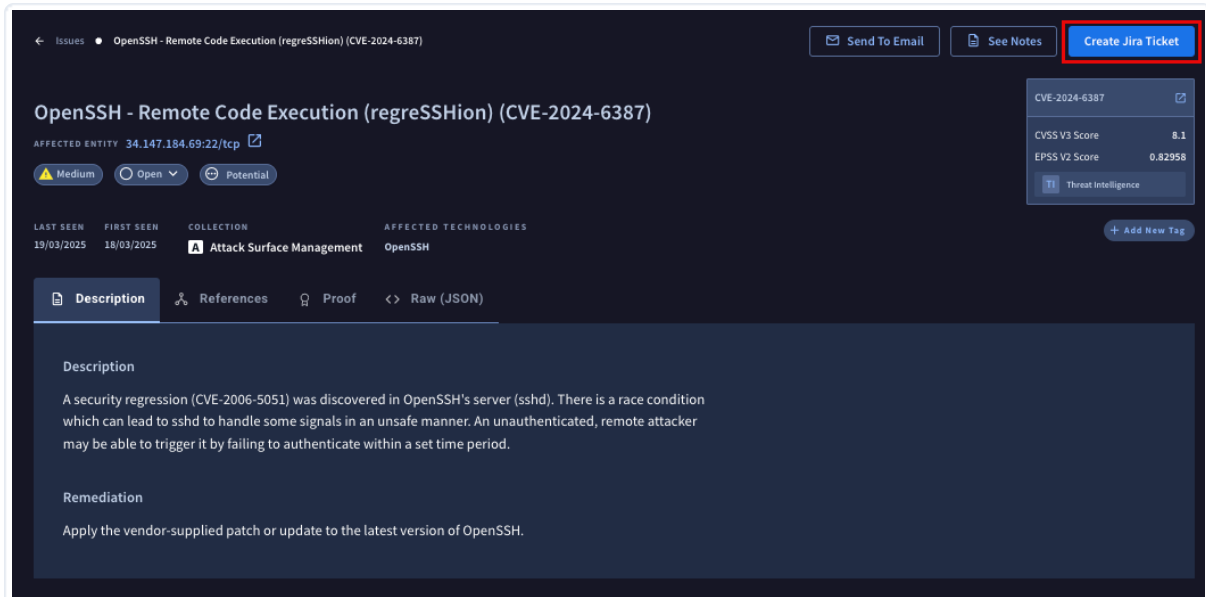
5. Click **Connect**.

### Create Jira ticket



This integration requires the **Task** issue type to be configured within the target Jira project.

1. Once integrated, navigate to the MA-ASM **Issues** page, and then select an Issue.
2. Click **Create Jira Ticket**.



Issues • OpenSSH - Remote Code Execution (regreSSHion) (CVE-2024-6387)

Send To Email See Notes **Create Jira Ticket**

### OpenSSH - Remote Code Execution (regreSSHion) (CVE-2024-6387)

AFFECTED ENTITY 34.147.184.69:22/tcp

Medium Open Potential

CVSS V3 Score 8.1  
EPSS V2 Score 0.82958  
Threat Intelligence

LAST SEEN 19/03/2025 FIRST SEEN 18/03/2025 COLLECTION Attack Surface Management AFFECTED TECHNOLOGIES OpenSSH

Add New Tag

Description References Proof Raw (JSON)

**Description**

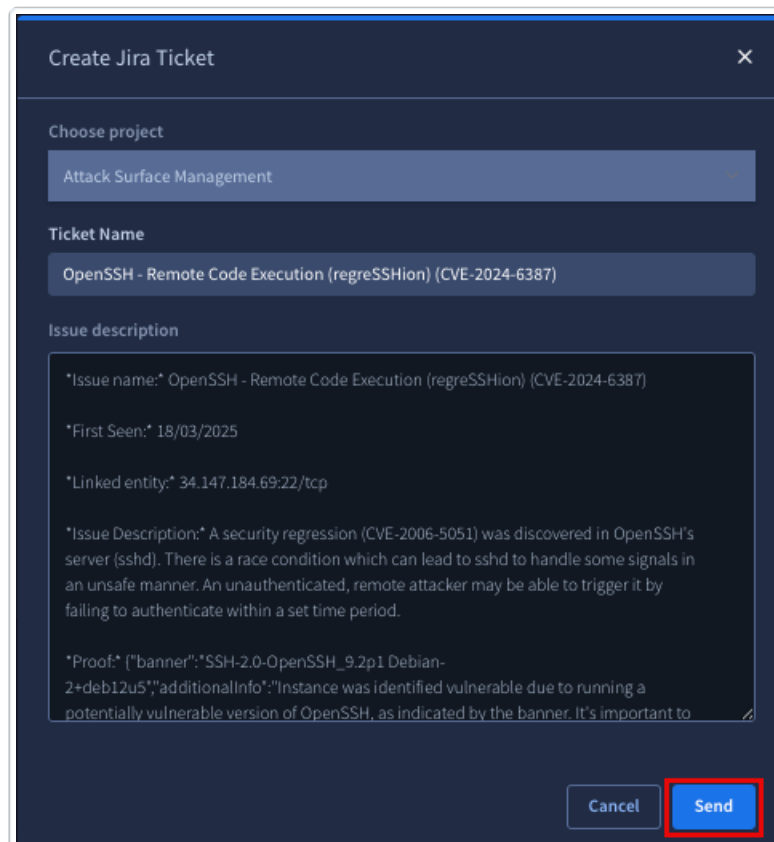
Description

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

**Remediation**

Apply the vendor-supplied patch or update to the latest version of OpenSSH.

3. Choose a project in Jira and click **Send**.



Create Jira Ticket

Choose project

Attack Surface Management

**Ticket Name**

OpenSSH - Remote Code Execution (regreSSHion) (CVE-2024-6387)

**Issue description**

\*Issue name:\* OpenSSH - Remote Code Execution (regreSSHion) (CVE-2024-6387)

\*First Seen:\* 18/03/2025

\*Linked entity:\* 34.147.184.69:22/tcp

\*Issue Description:\* A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

\*Proof:\* {"banner": "SSH-2.0-OpenSSH\_9.2p1 Debian-2+deb12u5", "additionalInfo": "Instance was identified vulnerable due to running a potentially vulnerable version of OpenSSH, as indicated by the banner. It's important to"}/

Cancel **Send**

The Jira ticket is visible in the MA-ASM Issue view.

Issues • OpenSSH - Remote Code Execution (regreSSHion) (CVE-2024-6387) Send To Email See Notes

## OpenSSH - Remote Code Execution (regreSSHion) (CVE-2024-6387)

AFFECTED ENTITY [34.147.184.69:22/tcp](#)

Medium Open Potential

| LAST SEEN  | FIRST SEEN | COLLECTION                         | AFFECTED TECHNOLOGIES |
|------------|------------|------------------------------------|-----------------------|
| 19/03/2025 | 18/03/2025 | <b>A</b> Attack Surface Management | OpenSSH               |

TI Threat Intelligence + Add New Tag

**Description** | References | Proof | Raw (JSON)

**Description**

A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead to sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.

**Remediation**

Apply the vendor-supplied patch or update to the latest version of OpenSSH.

**JIRA Tickets** Create Jira Ticket

<https://attacksurface.atlassian.net/browse/...>

PROJECT  
**Attack Surface Management**

CREATED  
19/03/2025 09:32