How a New HackerOne Integration with AWS Security Hub Accelerates Vulnerability Remediation Time

HackerOne

August 25th, 2021

SHARE

Today, HackerOne announced an integration with AWS Security Hub that exchanges vulnerability findings and streamlines workflows to accelerate security actions. The integration consolidates and routes vulnerability intelligence from HackerOne to AWS Security Hub, delivering greater visibility into crucial gaps that could lead to a cyberattack.

AWS Security Hub combines security alerts and intelligence from AWS and partner security products into a single view, enabling AWS customers to streamline their cloud security operations.

How Can You Use the Integration?

This new integration reduces the manual processes of comparing and taking action on vulnerability findings between the two platforms with workflow automation. AWS customers can use the integration to:

- **Aggregate and prioritize vulnerabilities from HackerOne in Security Hub:** Sync all HackerOne vulnerability findings and use AWS Security Hub as the single console to manage and prioritize those findings.
- **Forward findings from Security Hub and other partners to HackerOne:** Compare AWS Security Hub findings with those found in reports from HackerOne to see duplicates and finding status.

The HackerOne community of ethical hackers finds vulnerabilities, generates reports, and triages all findings to reduce the time to remediation and lockdown exploitable vectors. Once HackerOne has validated and prioritized a vulnerability report, customers using the AWS Security Hub and HackerOne integration will receive new vulnerability findings via a continuous workflow, as shown in Figure 1 below.

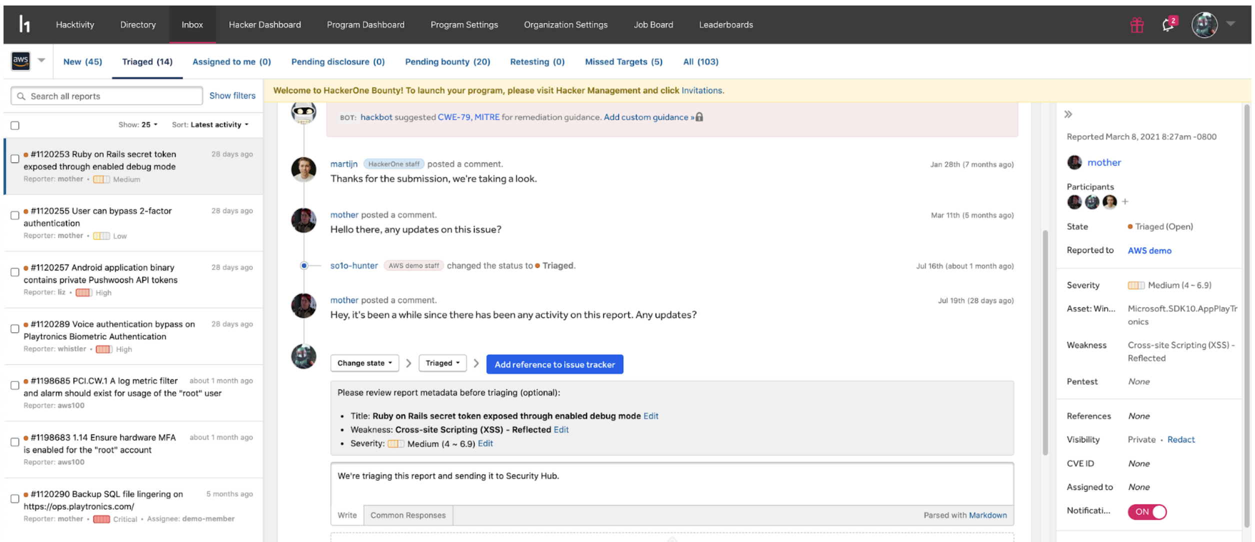

Figure 1: The integration workflow includes the vulnerability search, report, triage, validation, and notification process

The integration will automatically push HackerOne reports to AWS Security Hub. The findings in AWS Security Hub will show severity, status, description, and more to provide security teams with the context needed to make informed decisions.

Teams can compare Security Hub's findings with reports from HackerOne to identify and remove duplicates without switching between multiple consoles, as shown in Figure 2 below.

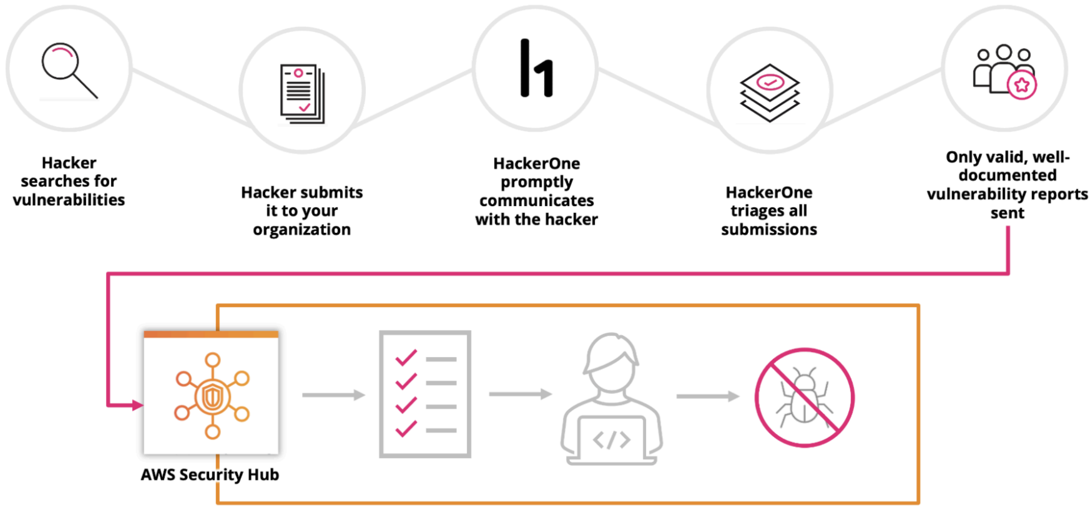

Figure 2: Comparison of Security Hub findings with HackerOne reports

Report resolution status originating in HackerOne but presented in Security Hub is automatically updated in Security Hub, avoiding manually verifying the resolution in a separate action, as shown in Figure 3 below.

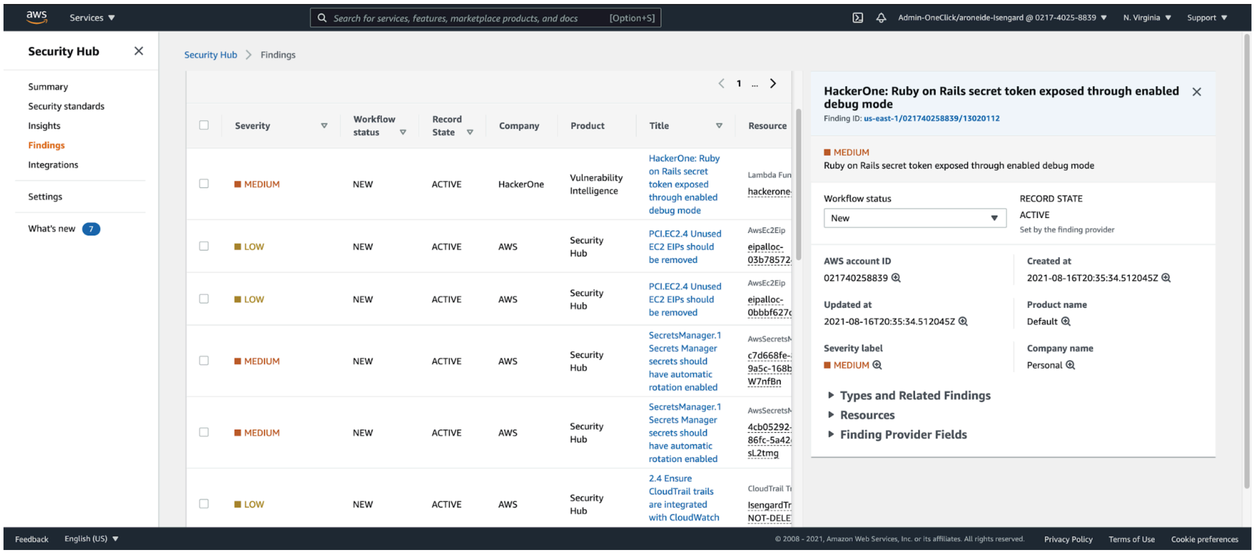

Figure 3: Report resolution between HackerOne and AWS Security Hub

In addition, any change made to a Security Hub report will trigger an event that syncs all changes back to HackerOne, eliminating errors and saving time.

Security Hub can also forward findings to HackerOne, allowing customers to use the HackerOne platform to centrally manage both Security Hub findings and the vulnerabilities found by the HackerOne community. To provide additional context to the analysts using HackerOne, customers can click on the “Send to HackerOne” button in the Security Hub interface, as seen below in Figure 4.

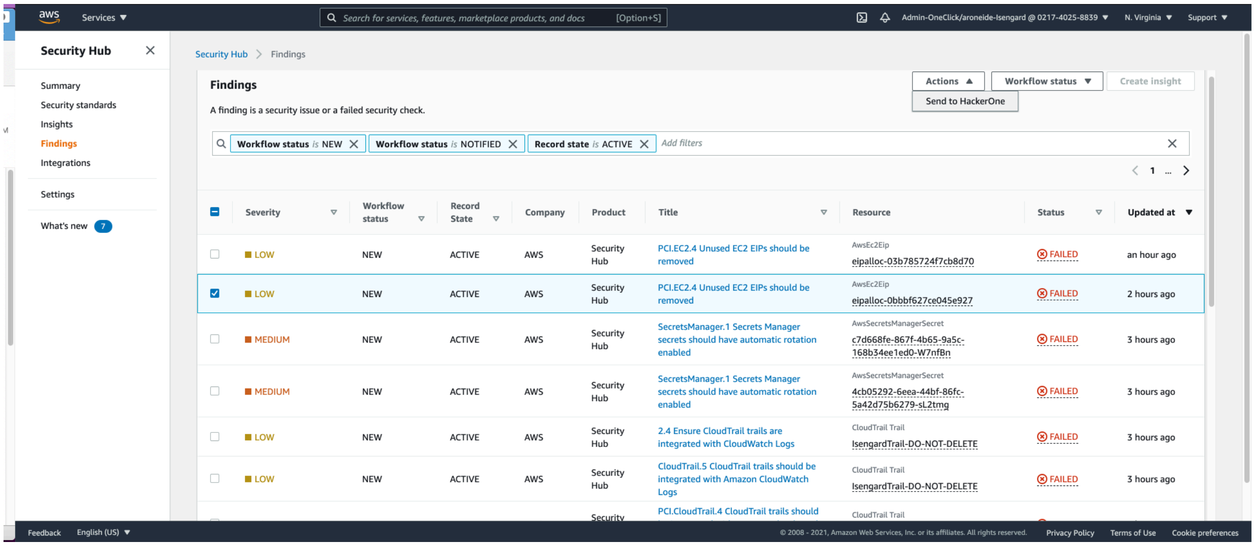

Figure 4: Sending Security Hub findings to HackerOne

Once synced, customers can use the HackerOne platform to manage the finding workflow. They can filter synced Security Hub reports via the HackerOne Inbox, then triage, escalate, and resolve issues. Finally, they can request retests to validate fixes, ensuring proper resolution of issues.

The workflow integration between HackerOne and AWS Security Hub is easy to configure and ensures vulnerability findings reach the right people at the right time with the right status. Security teams need workflows that save time, improve efficiencies, and mitigate risk. Automating the workflows around hacker-powered vulnerability intelligence in AWS Security Hub helps security teams become more efficient. To learn more about HackerOne and AWS Security Hub, visit the HackerOne and AWS page.