Synack

DATASHEET

On-Demand Testing for Zero Day Vulnerabilities and CVEs

Guaranteed testing coverage for pressing vulnerabilities like Log4j and Spring4Shell

Through the Synack Platform, you can activate Synack Red Team (SRT) researchers to perform on-demand, targeted testing of certain common vulnerabilities and exposures (CVE). This will produce proof-of-coverage reports that detail testing methodologies.

Exploitable findings will also populate the vulnerabilities tab within the Synack Platform, enabling a vulnerability management/remediation workflow.

Same day zero day response

When a new zero day appears, it becomes available in the Synack Platform within hours for immediate testing by skilled members of the SRT. You can activate the testing and receive results all within the same platform. Additionally, any CVE that doesn't already exist in the catalog can be requested. To reduce time to test, credits can be purchased in advance to be redeemed for urgent requests like a zero day.

Reporting for proof of coverage and work

When SRT researchers check for a CVE, they document their techniques with written reports and screenshots. Their work, along with their vulnerability findings, are quickly made accessible in-platform.

For convenience, CVE testing, along with other tasks performed by the SRT, can be exported to a PDF format for sharing with executive audiences and other stakeholders.

How it works

A new zero day (like log4j) appears

The CVE is added to the catalog in-platform within hours

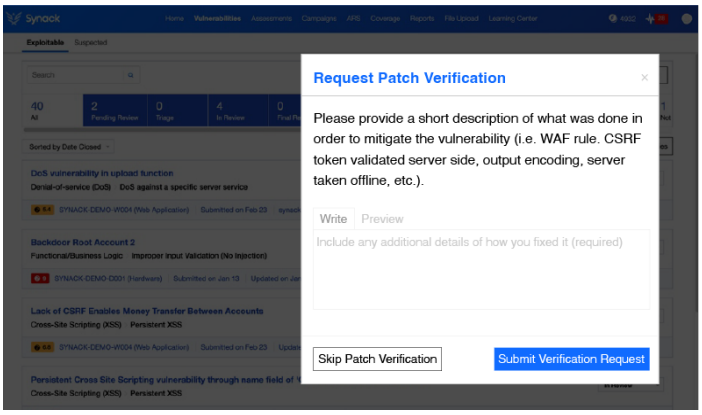
The Synack Red Team tests across your assets

Reports detail methodology and status

Finding the vulnerabilities that matter

Even if no exploitable vulnerabilities are found, you will receive written reports on the testing performed. However, when vulnerabilities are found, they are triaged by internal Synack Operations teams and presented in-platform.

Through the Synack Platform's vulnerability management workflow, you can access details on exploitable findings (including screenshots), communicate with researchers on methodologies and patching and request patch verification for retesting.



Test ahead of scanners with human-led testing

Often, scanners will be able to detect zero days and critical CVEs after a few days, or even weeks, when a signature for the vulnerability is defined and implemented. This is already too late when we know malicious actors begin scanning for vulnerabilities 15 minutes after they've been released.

Through the Synack Platform, you can test within a few hours of the zero day becoming known, through human-led testing from the Synack Red Team.

The best CVE testing methodologies

SRT members from around the world begin collaborating on exploit techniques hours after a zero day becomes known.

With a tightly knit community of diverse researchers from around the world, you can be sure that researchers are using the latest up-to-the-minute testing techniques for a given vulnerability.

More on CVEs

CVE uses the Common Vulnerability Scoring System (CVSS) to assign a severity value to each vulnerability. It is a metric displayed within the Synack Platform. The wide range of CVSS scores assigned to vulnerabilities reflects the broad array of potential consequences — everything from directory traversal to remote code execution. While thousands of vulnerabilities are identified by CVE each year, the ones that make the news often have higher CVSS scores.