HORIZON3.ai

~~TRUST BUT~~ VERIFY

WHITE PAPER

Rapid Response

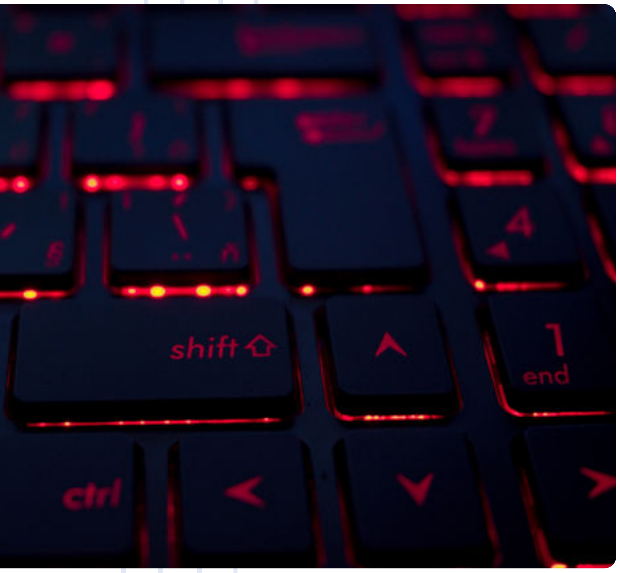
Fix What Matters: Accelerating Cyber Defense Through the Eyes of an Attacker

Fix What Matters: Accelerating Cyber Defense Through the Eyes of an Attacker

How Horizon3.ai's Rapid Response Empowers Organizations to Outpace Emerging Cyber Threats

The emergence of new attack vectors, the steady growth of attack surfaces, and the increasing speed at which vulnerabilities are exploited underscore the critical need for proactive defense strategies. As such, the speed at which organizations can identify, assess, and mitigate emerging threats directly impacts their resilience against cyberattacks.

In this white paper, we delve into the critical importance of responding to exploitable vulnerabilities in their nascent stages and describe how Horizon3.ai's one-of-a-kind Rapid Response service provides NodeZero™ customers a strategic advantage by providing early, actionable intelligence to counteract emerging threats that have been identified in their organizations' assets.



Understanding the Threat Landscape

While defenders are often hyper-focused on the esoteric suite of security tools within their organizations, attackers have a lower threshold to impact since they only need to break in once, whether it be exploiting a zero-day or N-day vulnerability, taking advantage of misconfigurations, or even capitalizing on weak/compromised credentials.

Cyber threats evolve rapidly, driven by the ingenuity and persistence of malicious actors. From sophisticated nation-state attacks to opportunistic cybercriminals, organizations face a wide range of adversaries seeking to exploit vulnerabilities for financial gain, espionage, or simply, disruption. At the same time, defenders must be proactive in identifying emerging vulnerabilities and subsequently prioritizing mitigation efforts for what is exploitable, not just vulnerable, within their unique environments before the attackers do. With noise in the cyber industry at an all-time high, new attack surfaces being introduced every day, and the number of potential vulnerabilities rising at unprecedented speeds, it is more important now than ever to utilize offensive strategies to find, fix, and verify defensive postures.

The Need for Speed in Cyber Defense

There are only a handful of scenarios that require all other projects to be put on pause with all-hands-on-deck: an in-progress cyberattack, IT outages that interrupt business operations, and emerging attacks verified to be relevant and negatively impactful to the specific organization.

The window of time between the public disclosure of a vulnerability and its exploitation in the wild is steadily shrinking, and with many zero-day vulnerabilities being exploited before public disclosures, a quick reaction and laser-focused attention on exploits that matter are pivotal to the success of any security team.

Equipped with the latest advancements in artificial intelligence and machine learning algorithms, attackers are quicker than ever to capitalize on newly discovered weaknesses, making swift action for critical vulnerabilities essential for effective cyber defense. This trend is underscored by Mandiant's recent report on time-to-exploit trends which highlights the increasing speed at which vulnerabilities are being weaponized by threat actors, often exploiting them within hours or days of public disclosure.[1]

As the future of cyber warfare will be a battle between machines and algorithms, organizations must be able to filter through the noise of vulnerability announcements and focus their remediation efforts on vulnerabilities that are proven to be exploitable in their own environments. Without this knowledge, organizations have little other choice than to patch all known vulnerabilities regardless of whether it is exploitable or not—a task as impossible as it is unnecessary.

The effort that is required to execute a time-sensitive decision to prioritize an emerging threat at comparable speeds to real-world attackers requires consistent and advanced threat intelligence and research, meticulous cross-referencing between the organization's technology stack and affected versions, dedicated resources to exploit research and development, and an extended remediation effort depending on the vendor's recommended fix actions. Typically, by the time an organization has completed this work, they have already missed the window of opportunity to find affected assets and fix them before attackers begin to scrape the internet for publicly accessible exploitable targets.

Cybersecurity Infrastructure & Security Agency (CISA) Directive BOD 22-01 also supports the need for speed as **less than 4% of all CVEs have ever been exploited in the wild,** with **42% of these exploitations occurring on Day 0** of public disclosure.[2]

[1] https://www.mandiant.com/resources/blog/time-to-ex2loit-trends-2021-2022

[2] https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

Enter Horizon3.ai's Rapid Response

Recognizing the critical role of response times in emerging exploits in the wild, Horizon3.ai's Rapid Response is offered as a service included with NodeZero.

At the heart of Rapid Response is the notion that early detection using the attackers' perspective and quick reaction from the defenders' perspective is essential to staying ahead of evolving cyberattacks before they are trending and a critical element of a successful cybersecurity program.

By leveraging Horizon3.ai's expertise in offensive security and NodeZero's autonomous pentesting capabilities, Rapid Response empowers defenders by providing them with early verified threat intelligence. Work is done by Horizon3.ai to assess the exploitability and urgency of these nascent stage vulnerabilities, considering factors such as ease of exploitation, severity of impact, and the prevalence of use.

Horizon3.ai has had a proven track record of disclosing major exploitable vulnerabilities to its customers well before they are exploited in the wild or even get added to major vulnerability catalogs like MITRE CVE and CISA's Known Exploited Vulnerabilities (CISA KEVs) catalog.

NodeZero's Rapid Response Center

With Horizon3.ai's continued commitment to inform and equip defenders as quickly as possible with the right intelligence and tools to succeed, comes the latest version of NodeZero including the new Rapid Response center—a one-stop shop for emerging threats.

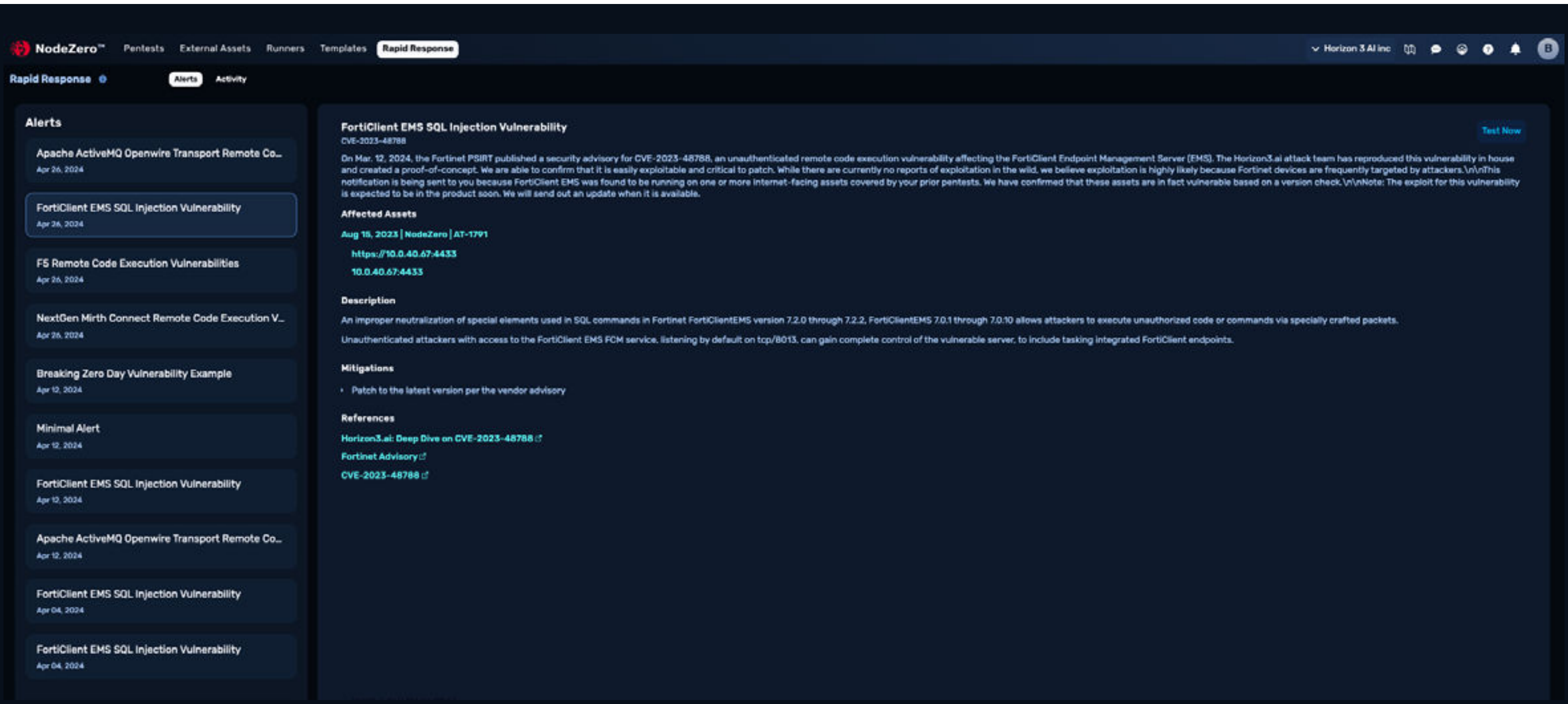
When addressing a threat anticipated to be widely exploited, Horizon3.ai's Attack Team will either develop a proof of concept (POC) exploit in-house or enhance existing public POCs to integrate them into NodeZero as new attack content.

Organizations using the Rapid Response service benefit from both priority and tailored threat alerts. During a Rapid Response alert, Horizon3.ai's Attack Team manually attempts benign exploitations of each potentially vulnerable asset across all NodeZero customers, limiting their scope to assets previously tested and seen in NodeZero.

Regardless of whether an official patch is available, and even if the exploit itself is not yet available in the NodeZero product, any assets verified as exploitable will then be highlighted in the new Rapid Response center, with details about which test the asset was seen in, the IP, hostname, or domain of the affected asset(s), along with the current mitigation or remediation recommendations, all updated in real-time as the threat develops (See Figure 1 on the next page).

Once a test for the exploit is added to NodeZero, Horizon3.ai customers can launch tests from the Rapid Response center or the Rapid Response modal in ‘Run Pentest’ to verify successful mitigation or check for exploitability against other assets not tested by the Horizon3.ai Attack Team (Figure 2). For the most comprehensive assessment of impact and security validation, users can also run a full internal and external pentest against the entire digital infrastructure, which automatically includes the latest NodeZero exploits.

▼ ***Figure 1***
Rapid Response alerts detail which assets in your organization were verified as exploitable.



Alerts

Apache ActiveMQ Openwire Transport Remote Co...
Apr 26, 2024

FortiClient EMS SQL Injection Vulnerability
Apr 26, 2024

F5 Remote Code Execution Vulnerabilities
Apr 26, 2024

NextGen Mirth Connect Remote Code Execution V...
Apr 26, 2024

Breaking Zero Day Vulnerability Example
Apr 12, 2024

Minimal Alert
Apr 12, 2024

FortiClient EMS SQL Injection Vulnerability
Apr 12, 2024

Apache ActiveMQ Openwire Transport Remote Co...
Apr 12, 2024

FortiClient EMS SQL Injection Vulnerability
Apr 04, 2024

FortiClient EMS SQL Injection Vulnerability
Apr 04, 2024

FortiClient EMS SQL Injection Vulnerability
CVE-2023-48788

On Mar. 12, 2024, the Fortinet PSIRT published a security advisory for CVE-2023-48788, an unauthenticated remote code execution vulnerability affecting the FortiClient Endpoint Management Server (EMS). The Horizon3.ai attack team has reproduced this vulnerability in house and created a proof-of-concept. We are able to confirm that it is easily exploitable and critical to patch. While there are currently no reports of exploitation in the wild, we believe exploitation is highly likely because Fortinet devices are frequently targeted by attackers.\n\nThis notification is being sent to you because FortiClient EMS was found to be running on one or more internet-facing assets covered by your prior pentests. We have confirmed that these assets are in fact vulnerable based on a version check.\n\nNote: The exploit for this vulnerability is expected to be in the product soon. We will send out an update when it is available.

Affected Assets

Aug 15, 2023 | NodeZero | AT-1791
https://10.0.40.67:4433
10.0.40.67:4433

Description

An improper neutralization of special elements used in SQL commands in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attackers to execute unauthorized code or commands via specially crafted packets.

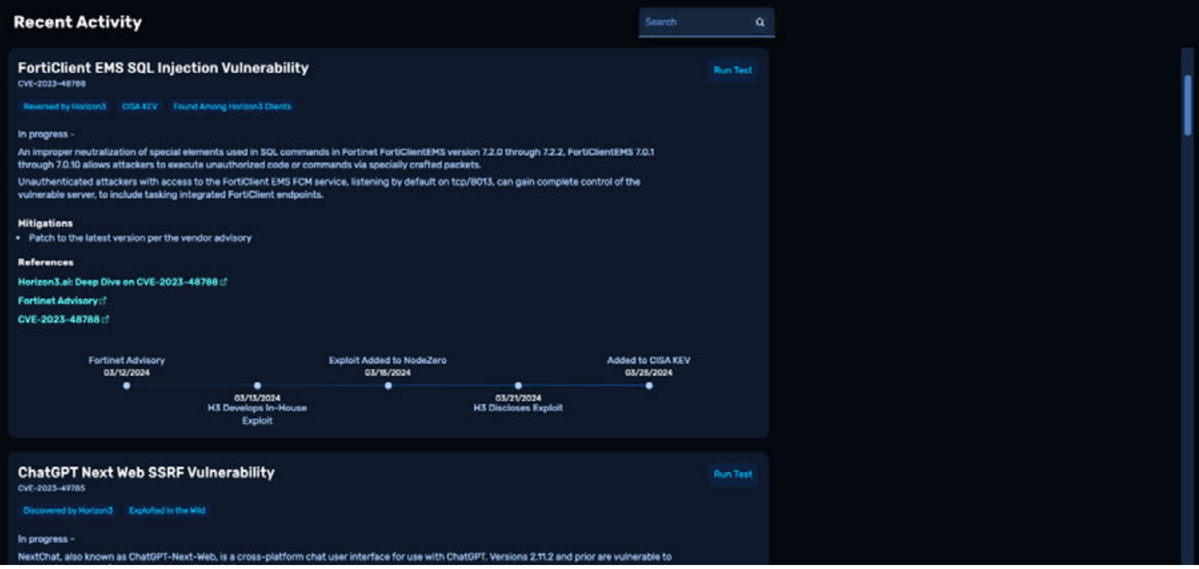
Unauthenticated attackers with access to the FortiClient EMS FCM service, listening by default on tcp/8013, can gain complete control of the vulnerable server, to include tasking integrated FortiClient endpoints.

Mitigations

- Patch to the latest version per the vendor advisory

References

Horizon3.ai: Deep Dive on CVE-2023-48788
Fortinet Advisory
CVE-2023-48788



Recent Activity

FortiClient EMS SQL Injection Vulnerability
CVE-2023-48788

In progress -

An improper neutralization of special elements used in SQL commands in Fortinet FortiClientEMS version 7.2.0 through 7.2.2, FortiClientEMS 7.0.1 through 7.0.10 allows attackers to execute unauthorized code or commands via specially crafted packets.

Unauthenticated attackers with access to the FortiClient EMS FCM service, listening by default on tcp/8013, can gain complete control of the vulnerable server, to include tasking integrated FortiClient endpoints.

Mitigations

- Patch to the latest version per the vendor advisory

References

Horizon3.ai: Deep Dive on CVE-2023-48788
Fortinet Advisory
CVE-2023-48788

Fortinet Advisory 03/12/2024
03/13/2024 H3 Develops In-House Exploit
Exploit Added to NodeZero 03/15/2024
03/21/2024 H3 Discloses Exploit
Added to CISA KEV 03/25/2024

ChatGPT Next Web SSRF Vulnerability
CVE-2023-49785

In progress -

NextChat, also known as ChatGPT-Next-Web, is a cross-platform chat user interface for use with ChatGPT. Versions 2.11.2 and prior are vulnerable to

▲ ***Figure 2***
From the Activity tab of the Rapid Response center, users can track timelines, access details, mitigation recommendations, and research references, and even launch targeted tests for the latest emerging threats.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Advantages of the Rapid Response Service

1. Advisory of Exploitation in the Wild:

Committed to the shared mission of cybersecurity, all NodeZero users automatically benefit from the Rapid Response service. Through the expertise of Horizon3.ai's team of former US nation-state attackers and exploit developers, NodeZero users receive tailored alerts of emerging exploitable vulnerabilities.

This early warning augments defenders' existing threat intelligence capabilities and enables them to stay informed and assess and mitigate potential risks relative to their organization before they can be exploited by malicious actors. With a timeline provided for each emerging threat in the Rapid Response center, defenders can quickly get answers to the what, why, and so-what of threat intelligence.

2. Tailored Exploitability Validation and Impact Assessments:

Alerts that surface through the Rapid Response cycle go beyond a high-level notice of potential vulnerabilities. Each Rapid Response alert discloses details about specific assets within each organization's digital infrastructure that were manually verified by the Horizon3.ai Attack Team as being exploitable, not just vulnerable, to emerging threat trends. By providing a comprehensive analysis of the real impact of an unknown threat, Horizon3.ai continues to reinforce with its customers the importance of using the attacker's perspective to evaluate risk and priority.

NodeZero users leverage the Rapid Response service's proactive exploitations to reclaim crucial time in responding to emerging attacks, leveraging Horizon3.ai as a partner to expand their insight into unknown or undisclosed threats. As these manual evaluations are limited in scope to assets previously seen in the NodeZero portal, customers are urged to conduct regular asset discoveries on external assets to maximize the benefits of the latest threat research and ensure exploitability evaluations are being completed against the most up-to-date assets for their organization. Consistent visibility through NodeZero enhances the Attack Team's ability to assess the threat's impact comprehensively.

Customers who choose not to benefit from the custom alerts with proactive exploitability checks against public-facing assets may opt-out from their user settings in the NodeZero portal.

3. Access to Real-World Exploits:

One of the most unique aspects of the Rapid Response service is its provision of actual exploits modified to be safe to run in production, either developed as a part of original research from Horizon3.ai's Attack Team or reverse-engineered based on third-party research. Organizations unlock access to exploits days, weeks, and sometimes even months ahead of what is available to the rest of the industry.

This unprecedented access allows Horizon3.ai customers to self-test through actual exploitation, often before detection models are available, and calculate the impact unique to their organization, verify remediation efforts, and ensure that their digital assets remain secure against real-world threats ahead of known exploitation-in-the-wild. All historic Rapid Response cycles, along with their tests and timelines, can be accessed by any NodeZero user from either the 'Activity' tab within the Rapid Response center or the Rapid Response testing modal.

HORIZON3.ai
~~TRUST BUT~~ VERIFY

Qualifying a Rapid Response

Utilizing a combination of threat intelligence and subject matter expertise, Horizon3.ai's Attack Team prioritizes vulnerabilities through a process designed to optimize the speed of reaction during the small window of opportunity between public disclosure and known exploitation.

While Horizon3.ai's original zero-day findings follow a distinct workflow emphasizing responsible vendor disclosure first, N-day research is primarily focused on using the attacker's perspective to identify exploitable vulnerabilities and emerging threats the Attack Team anticipates will be widely exploited by bad actors.

As the Rapid Response service is centered around fast action, if a vulnerability is determined to already be widely exploited and the window of opportunity was missed, the exploit may still be added to the product but not pushed through Rapid Response. The flow chart in Figure 3 shows the decision-making process used by the Horizon3.ai Attack Team when determining whether a vulnerability goes through the Rapid Response cycle.

Though not an exhaustive list, major considerations during the value and impact assessments include:

- **Does the vulnerability affect publicly accessible or externally facing assets?**
- **Is the vulnerable asset widely utilized by Horizon3.ai's customers?**
- **Is the vulnerable asset widely deployed globally?**
- **Is the vulnerability anticipated to be exploited in the wild?**
- **Is the vulnerability easy to exploit?**
- **What does successful exploitation lead to in terms of impact, privilege, or access?**

The Horizon3.ai Rapid Response Cycle

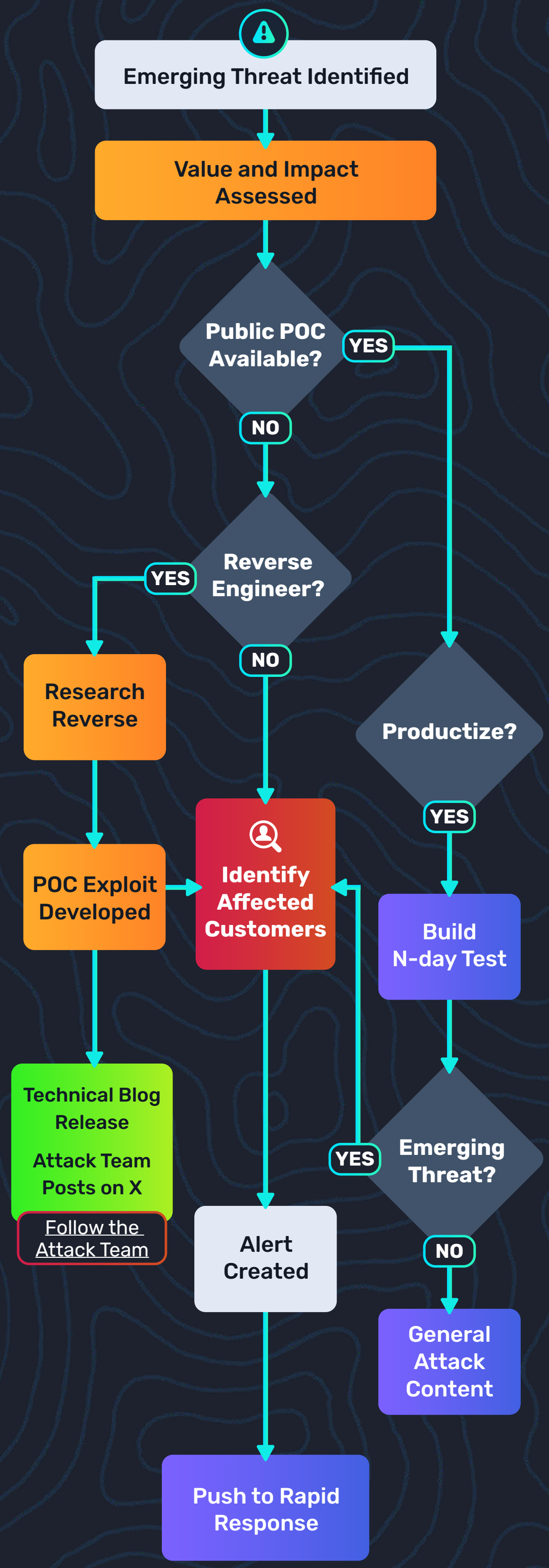
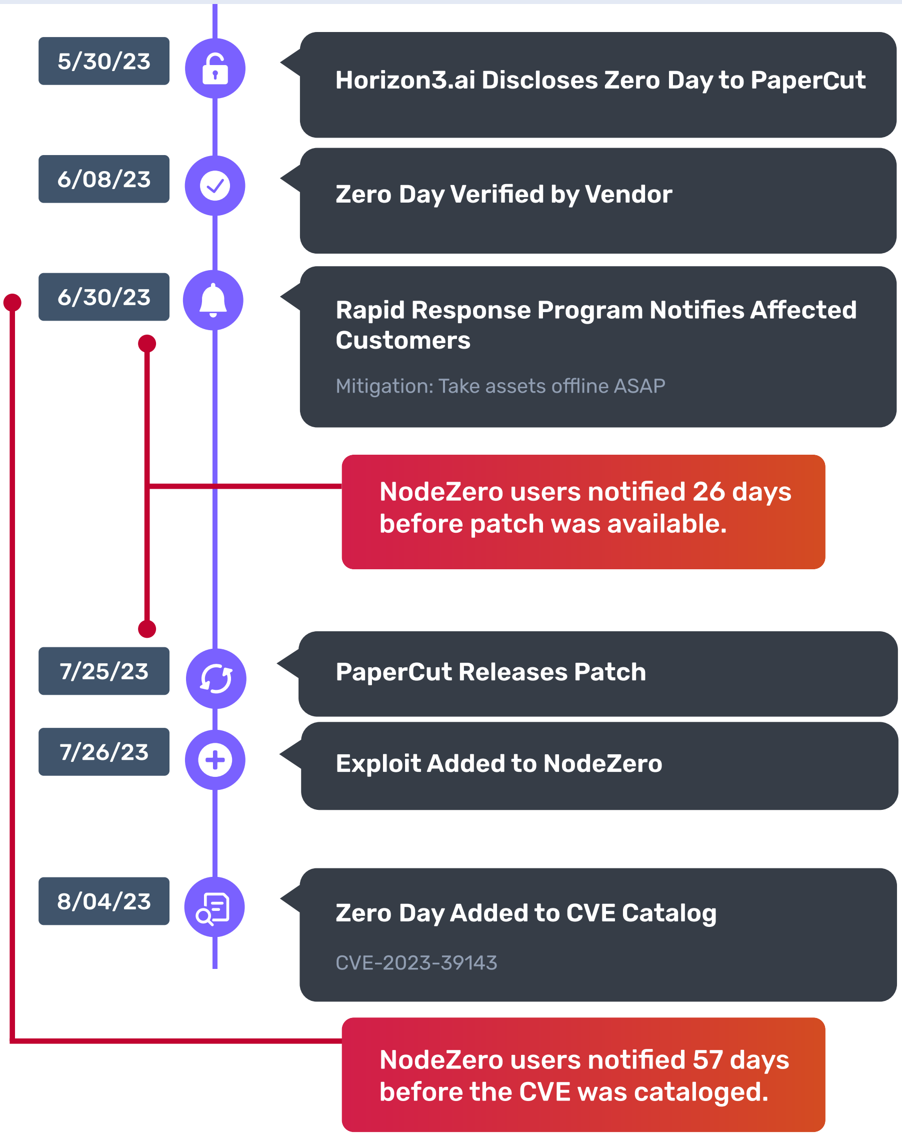


Figure 3

Rapid Response in Action

Zero Day: CVE-2023-39143 PaperCut Path Traversal/File Upload RCE



5/30/23 Horizon3.ai Discloses Zero Day to PaperCut

6/08/23 Zero Day Verified by Vendor

6/30/23 Rapid Response Program Notifies Affected Customers

Mitigation: Take assets offline ASAP

NodeZero users notified 26 days before patch was available.

7/25/23 PaperCut Releases Patch

7/26/23 Exploit Added to NodeZero

8/04/23 Zero Day Added to CVE Catalog

CVE-2023-39143

NodeZero users notified 57 days before the CVE was cataloged.

On May 30, 2023, Horizon3.ai privately disclosed details for a zero-day vulnerability to the vendor PaperCut. Following validation of the novelty of the remote code execution (RCE) vulnerability finding, in the interest of responsible public disclosure, Horizon3.ai worked closely with PaperCut to ensure they had all the information needed to fix the vulnerability and validate their approach from the eyes of an attacker.

On June 30, with agreement from PaperCut, Horizon3.ai's Rapid Response service sent out alerts to affected customers with lists of assets manually verified as exploitable by the Horizon3.ai Attack Team. With no official patch available, the proactive alert instructed defenders to take publicly accessible instances of PaperCut offline until the patch was released.

Figure 4
NodeZero customers were able to proactively mitigate, remediate, and verify remediation of the PaperCut zero day identified by Horizon3.ai long before it was cataloged as a CVE.

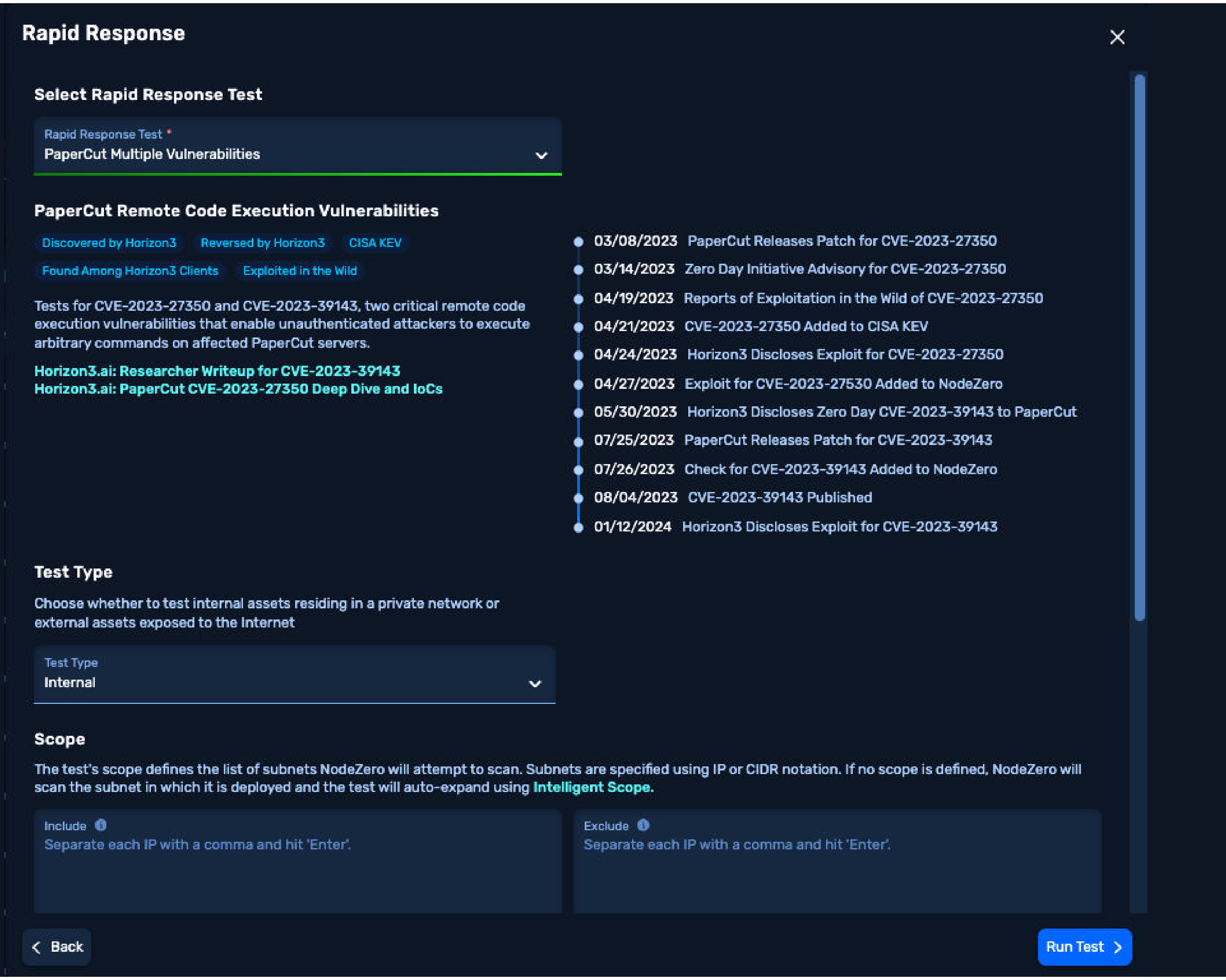
> "The security research team at Horizon3.ai carried out complex security research to identify two path traversal vulnerabilities which could be potentially leveraged to read and write arbitrary files. Direct server IP access is required. The Horizon3.ai team has worked with PaperCut to mitigate and validate our fixes.
>
> The PaperCut development team would like to thank Naveen and the research team at Horizon3.ai. We would like to acknowledge their sophisticated research methods as finding and demonstrating the issue required chaining multiple complex steps together. It is probably some of the most in-depth research that has ever been applied to PaperCut.[3]"

[3] https://www.papercut.com/kb/Main/securitybulletinjuly2023/#:~:text=Chained%20Path%20Traversal%20in%20Authenticated%20API%20(CVE%2D2023%2D39143)

Subsequently, on July 25, PaperCut publicly disclosed the zero-day vulnerability and released a patch.

As a result of the original research and the partnership with PaperCut, Horizon3.ai customers benefited from unique threat intelligence and attack content unavailable to anyone else in the world, having been notified of assets proven to be exploitable, a month before a patch was released. Even the handful of customers who had opted out of Rapid Response still benefitted from having the exploit added to NodeZero just one day after the patch was released by PaperCut and almost two weeks before the zero day was officially published as a CVE.

Kudos to the PaperCut team for going above and beyond in their response to our findings and engaging as a partner to fully understand and mitigate the vulnerability.



Rapid Response

Select Rapid Response Test

Rapid Response Test *
PaperCut Multiple Vulnerabilities

PaperCut Remote Code Execution Vulnerabilities

Discovered by Horizon3 · Reversed by Horizon3 · CISA KEV · Found Among Horizon3 Clients · Exploited in the Wild

Tests for CVE-2023-27350 and CVE-2023-39143, two critical remote code execution vulnerabilities that enable unauthenticated attackers to execute arbitrary commands on affected PaperCut servers.

Horizon3.ai: Researcher Writeup for CVE-2023-39143
Horizon3.ai: PaperCut CVE-2023-27350 Deep Dive and IoCs

03/08/2023 PaperCut Releases Patch for CVE-2023-27350
03/14/2023 Zero Day Initiative Advisory for CVE-2023-27350
04/19/2023 Reports of Exploitation in the Wild of CVE-2023-27350
04/21/2023 CVE-2023-27350 Added to CISA KEV
04/24/2023 Horizon3 Discloses Exploit for CVE-2023-27350
04/27/2023 Exploit for CVE-2023-27530 Added to NodeZero
05/30/2023 Horizon3 Discloses Zero Day CVE-2023-39143 to PaperCut
07/25/2023 PaperCut Releases Patch for CVE-2023-39143
07/26/2023 Check for CVE-2023-39143 Added to NodeZero
08/04/2023 CVE-2023-39143 Published
01/12/2024 Horizon3 Discloses Exploit for CVE-2023-39143

Test Type

Choose whether to test internal assets residing in a private network or external assets exposed to the Internet

Test Type
Internal

Scope

The test's scope defines the list of subnets NodeZero will attempt to scan. Subnets are specified using IP or CIDR notation. If no scope is defined, NodeZero will scan the subnet in which it is deployed and the test will auto-expand using Intelligent Scope.

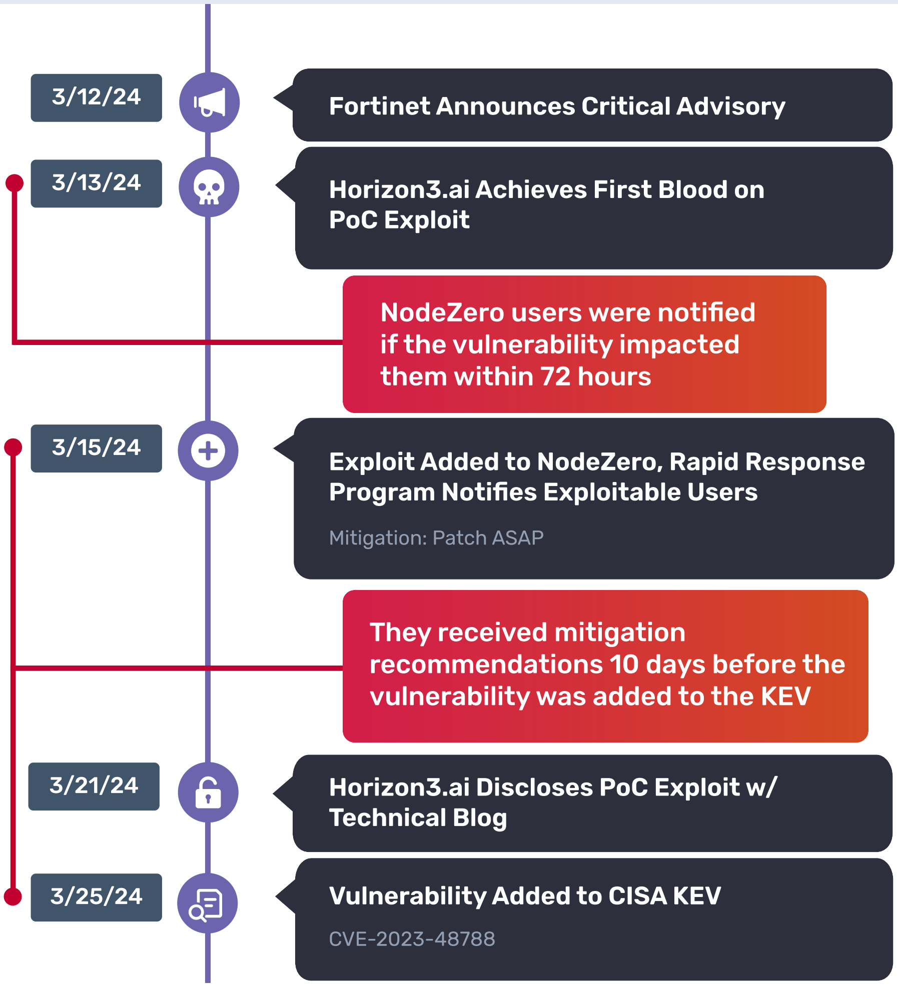
Include
Separate each IP with a comma and hit 'Enter'.

Exclude
Separate each IP with a comma and hit 'Enter'.

Figure 5
You can see the history of the PaperCut zero day in the Rapid Response center.

Rapid Response in Action

N-Day: CVE-2023-48788 FortiClient EMS SQL Injection



3/12/24 — Fortinet Announces Critical Advisory

3/13/24 — Horizon3.ai Achieves First Blood on PoC Exploit

NodeZero users were notified if the vulnerability impacted them within 72 hours

3/15/24 — Exploit Added to NodeZero, Rapid Response Program Notifies Exploitable Users

Mitigation: Patch ASAP

They received mitigation recommendations 10 days before the vulnerability was added to the KEV

3/21/24 — Horizon3.ai Discloses PoC Exploit w/ Technical Blog

3/25/24 — Vulnerability Added to CISA KEV

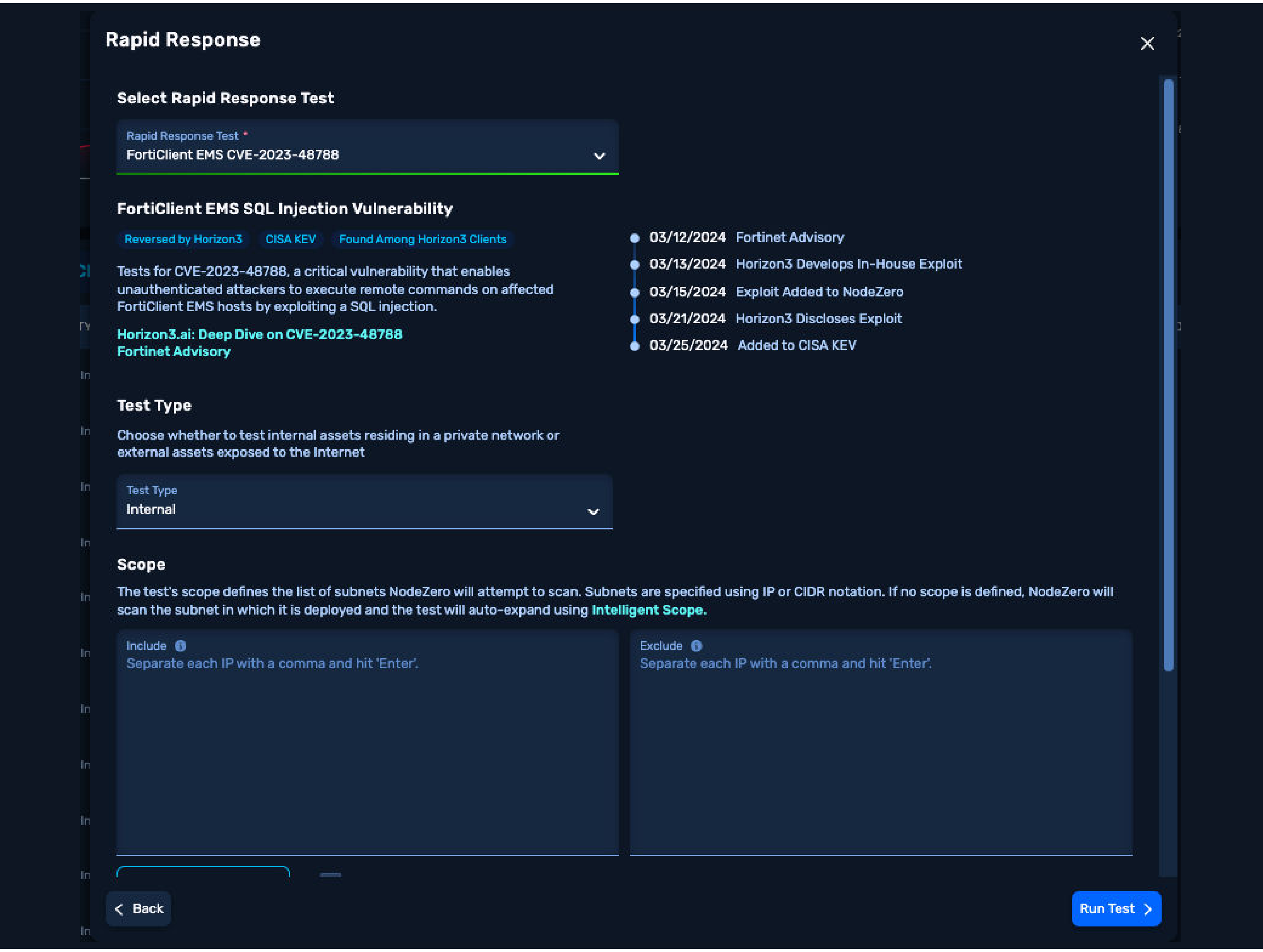
CVE-2023-48788

▲ ***Figure 6***
Horizon3.ai gets "first blood" on developing a PoC exploit for an N-day vulnerability.

On March 12, 2024, Fortinet issued a critical advisory regarding a structured query language (SQL) vulnerability of FortiClient Enterprise Management Server (EMS) that allows for unauthenticated code execution when exploited. Within 24 hours, Horizon3.ai's Attack Team was able to reverse-engineer the vulnerability and create the first known proof-of-concept exploit in the industry.

Within the first 72 hours of Fortinet's critical advisory, all Horizon3.ai customers were alerted of specific assets in their organizations that were manually exploitable alongside mitigation recommendations, nearly two weeks before the vulnerability was added to CISA's KEV Catalog.

Equipped with intelligence surrounding the vulnerability and a list of assets manually verified as exploitable by Horizon3.ai well before its disclosure on CISA KEV, customers were given a fighting chance before widespread exploitation. Without having to do any of the legwork, customers who were affected by this exploit were able to immediately prioritize the remediation of these specific validated targets, use the new FortiClient EMS test to run additional exploit checks on any additional potential targets not previously seen in NodeZero, and further test the infrastructure's overall health and exposure by running a more comprehensive internal and external pentest through NodeZero.



Rapid Response

Select Rapid Response Test

Rapid Response Test *
FortiClient EMS CVE-2023-48788

FortiClient EMS SQL Injection Vulnerability

Tests for CVE-2023-48788, a critical vulnerability that enables unauthenticated attackers to execute remote commands on affected FortiClient EMS hosts by exploiting a SQL injection.

Horizon3.ai: Deep Dive on CVE-2023-48788
Fortinet Advisory

- 03/12/2024 Fortinet Advisory
- 03/13/2024 Horizon3 Develops In-House Exploit
- 03/15/2024 Exploit Added to NodeZero
- 03/21/2024 Horizon3 Discloses Exploit
- 03/25/2024 Added to CISA KEV

Test Type

Choose whether to test internal assets residing in a private network or external assets exposed to the Internet

Test Type
Internal

Scope

The test's scope defines the list of subnets NodeZero will attempt to scan. Subnets are specified using IP or CIDR notation. If no scope is defined, NodeZero will scan the subnet in which it is deployed and the test will auto-expand using Intelligent Scope.

Include
Separate each IP with a comma and hit 'Enter'.

Exclude
Separate each IP with a comma and hit 'Enter'.

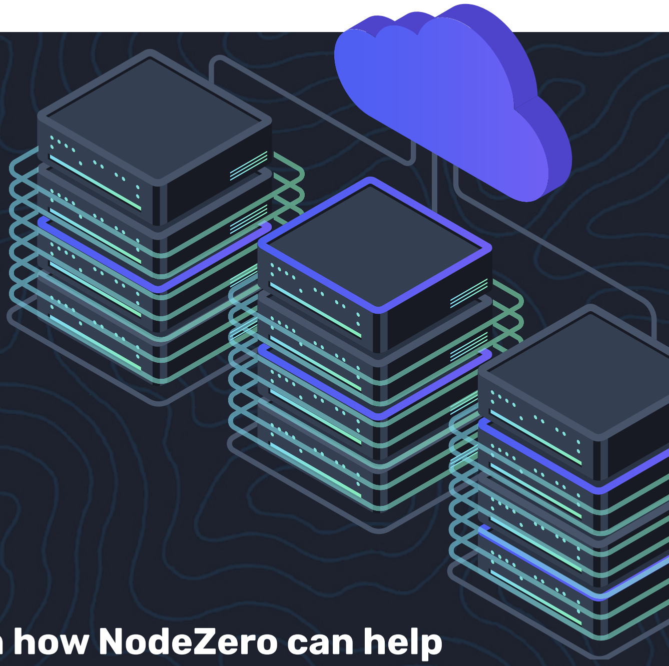
Figure 7
Stay up-to-date on the timeline of events of an N-day in NodeZero.

Conclusion

With the latest improvements to NodeZero, both new and existing customers now have a dedicated center for all Rapid Response activities, from self-service tests and threat details to alerts from Horizon3.ai of the exploitability of specific assets in their respective environments.

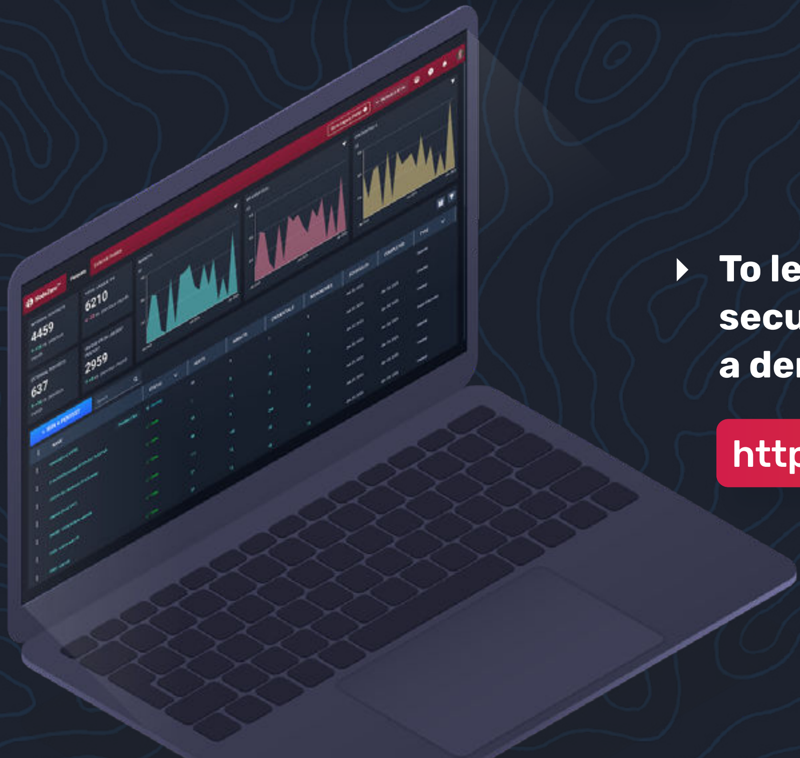
In today's dynamic threat landscape, speed is paramount followed closely by priority based on impact to business. By prioritizing velocity and providing tailored and actionable threat intelligence, Horizon3.ai's Rapid Response service uses offensive security principles to inform defenders about the targets that matter most when protecting critical infrastructure.

Empowering defenders to stay ahead of adversaries by cutting through industry noise, Horizon3.ai hopes to strengthen the security posture of all its customers and flip the script for blue teams, helping them to see what matters through the eyes of an attacker and prioritize accordingly.



- **To test drive NodeZero in your own environment, sign up for a free trial.**

https://www.horizon3.ai/trial



- **To learn how NodeZero can help secure your business, schedule a demo today.**

https://www.horizon3.ai/demo