Cyberint

Impactful Intelligence

CYBERINT ARGOS PLATFORM

VULNERABILITY INTELLIGENCE DATASHEET

Cyberint's CVE Intel module assigns a comprehensive risk score to each documented CVE and provides access to a library of open, deep and dark web intelligence on every vulnerability, allowing you to quickly understand the true risk profile of a given CVE and streamline prioritization for more a effective patch management program.

Challenge

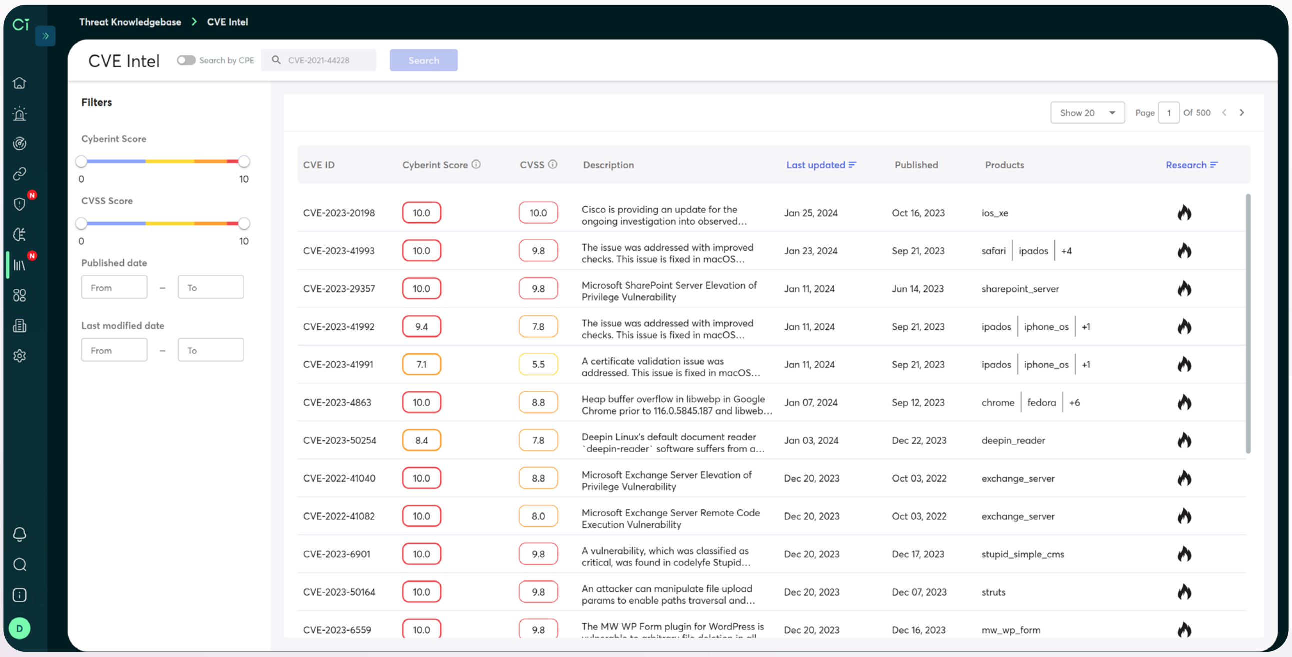
In 2023, over 28,000 new entries were added to the Common Vulnerabilities and Exposures (CVE) database, representing a 400% increase in new CVEs discovered annually in just 10 years. The exponential growth of software in enterprise environments, combined with a surge in CVE exploitation campaigns, has made vulnerability and patch management a difficult project. With limited resources available, security leaders face a challenge in deciding how to prioritize CVEs for remediation.

Solution

Cyberint's CVE Intel module leverages open, deep and dark web intelligence, as well as industry standard scoring systems such as CVSS and EPSS, to accurately assess the risk of each CVE. The Cyberint risk score takes relevant threat intelligence, such as the availability of exploit code and evidence that the CVE has been exploited in the wild, into account. Alerts are issued in real-time when a new CVE is published for a technology that is running on one of your external digital assets.

Key Benefits:

- Improve visibility on all the software running in your external attack surface
- Understand all the CVEs present in the software your organization is using
- Leverage threat intelligence to see which CVEs are discussed in threat actor forums, have POC code available, or are actively exploited in the wild
- Access a comprehensive and accurate risk score for every documented CVE
- Effectively prioritize CVEs to ensure optimal impact and risk reduction from your patch management program



CVE ID	Cyberint Score	CVSS	Description	Last updated	Published	Products	Research
CVE-2023-20198	10.0	10.0	Cisco is providing an update for the ongoing investigation into observed…	Jan 25, 2024	Oct 16, 2023	ios_xe	🔥
CVE-2023-41993	10.0	9.8	The issue was addressed with improved checks. This issue is fixed in macOS…	Jan 23, 2024	Sep 21, 2023	safari | ipados | +4	🔥
CVE-2023-29357	10.0	9.8	Microsoft SharePoint Server Elevation of Privilege Vulnerability	Jan 11, 2024	Jun 14, 2023	sharepoint_server	🔥
CVE-2023-41992	9.4	7.8	The issue was addressed with improved checks. This issue is fixed in macOS…	Jan 11, 2024	Sep 21, 2023	ipados | iphone_os | +1	🔥
CVE-2023-41991	7.1	5.5	A certificate validation issue was addressed. This issue is fixed in macOS…	Jan 11, 2024	Sep 21, 2023	ipados | iphone_os | +1	🔥
CVE-2023-4863	10.0	8.8	Heap buffer overflow in libwebp in Google Chrome prior to 116.0.5845.187 and libweb…	Jan 07, 2024	Sep 12, 2023	chrome | fedora | +6	🔥
CVE-2023-50254	8.4	7.8	Deepin Linux's default document reader `deepin-reader` software suffers from a…	Jan 03, 2024	Dec 22, 2023	deepin_reader	🔥
CVE-2022-41040	10.0	8.8	Microsoft Exchange Server Elevation of Privilege Vulnerability	Dec 20, 2023	Oct 03, 2022	exchange_server	🔥
CVE-2022-41082	10.0	8.0	Microsoft Exchange Server Remote Code Execution Vulnerability	Dec 20, 2023	Oct 03, 2022	exchange_server	🔥
CVE-2023-6901	10.0	9.8	A vulnerability, which was classified as critical, was found in codelyfe Stupid…	Dec 20, 2023	Dec 17, 2023	stupid_simple_cms	🔥
CVE-2023-50164	10.0	9.8	An attacker can manipulate file upload params to enable paths traversal and…	Dec 20, 2023	Dec 07, 2023	struts	🔥
CVE-2023-6559	10.0	9.8	The MW WP Form plugin for WordPress is	Dec 20, 2023	Dec 16, 2023	mw_wp_form	🔥

Cyberint

Understand The Software & Associated CVEs In Your Environment

Cyberint continuously and automatically discovers all your external IT assets, the technologies and version running on each asset, and any CVEs associated with the software you have deployed.

Gain Visibility On Technologies In Use

Discover your external attack surface and all of the software and services running on each of your Internet-facing assets.

Know Where Software Is Running

Keep an up-to-date inventory of technologies to understand what software is running and on which assets.

Get An Overview Of Relevant CVEs

Gain a complete overview of all the known CVEs in software running in your environment, as well as the risk scores.

Receive A Real-Time Alert When A New CVE Is Published

Cyberint issues an alert when an old technology with known CVEs is deployed on one of your assets or when a new CVE that affects a technology already running on one of your assets is published.

Stay Ahead Of Old Software & CVEs

Understand when an outdated software is deployed in your environment to know when new CVEs are introduced.

Know When A New CVE Is Revealed

Receive an alert when a new CVE is documented for a specific technology running on one of your external assets.

Stay Ahead of CVE Exploitation

Research the CVEs in your attack surface to know which have public exploit PoCs, which are exploited in the wild, and so on.

Effectively Prioritize CVEs To Reduce Risk & Prevent Breaches

Cyberint helps you to accurately and comprehensively understand the risk that each CVE creates for your organization, helping you to optimize remediation efforts, reduce cyber risk, and stay secure.

Quickly Eliminate Critical Risks

Understand which CVEs are creating the most risk for your organization so you can patch them immediately.

Prioritize CVEs To Optimize Resources

Make the most of the resources you invest in patch management with effective and optimal prioritization of CVEs.

Improve Hygiene & Stay Secure

Improve your patch and vulnerability management processes to strengthen security posture and prevent breaches.

> “Because we’re a small team, the Cyberint analysts are like an extension of us, which really helps from a risk management standpoint.”
>
> Evans Duvall, Cyber Security Engineer, Terex
>
> Read more in the customer case study.

> “We realized that Cyberint was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web.”
>
> Benjamin Bachmann, Head of Group Information Security, Ströer
>
> Read more in the customer case study.

> “Once we identified the need to address the risk of fraudulent websites and social profiles, I quickly realized we needed to handle this in a scalable manner. Our solution is to use Cyberint to help us automatically detect and takedown these threats.”
>
> Ken Lee, IT Risk and Governance Manager at Webull Technologies
>
> Read more in the customer case study.

Recognition As An Industry Leader From Trusted Analysts

Gartner. FROST & SULLIVAN IDC

Discover Cyberint with a personalized demo

About Cyberint

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform’s patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com

Cyberint