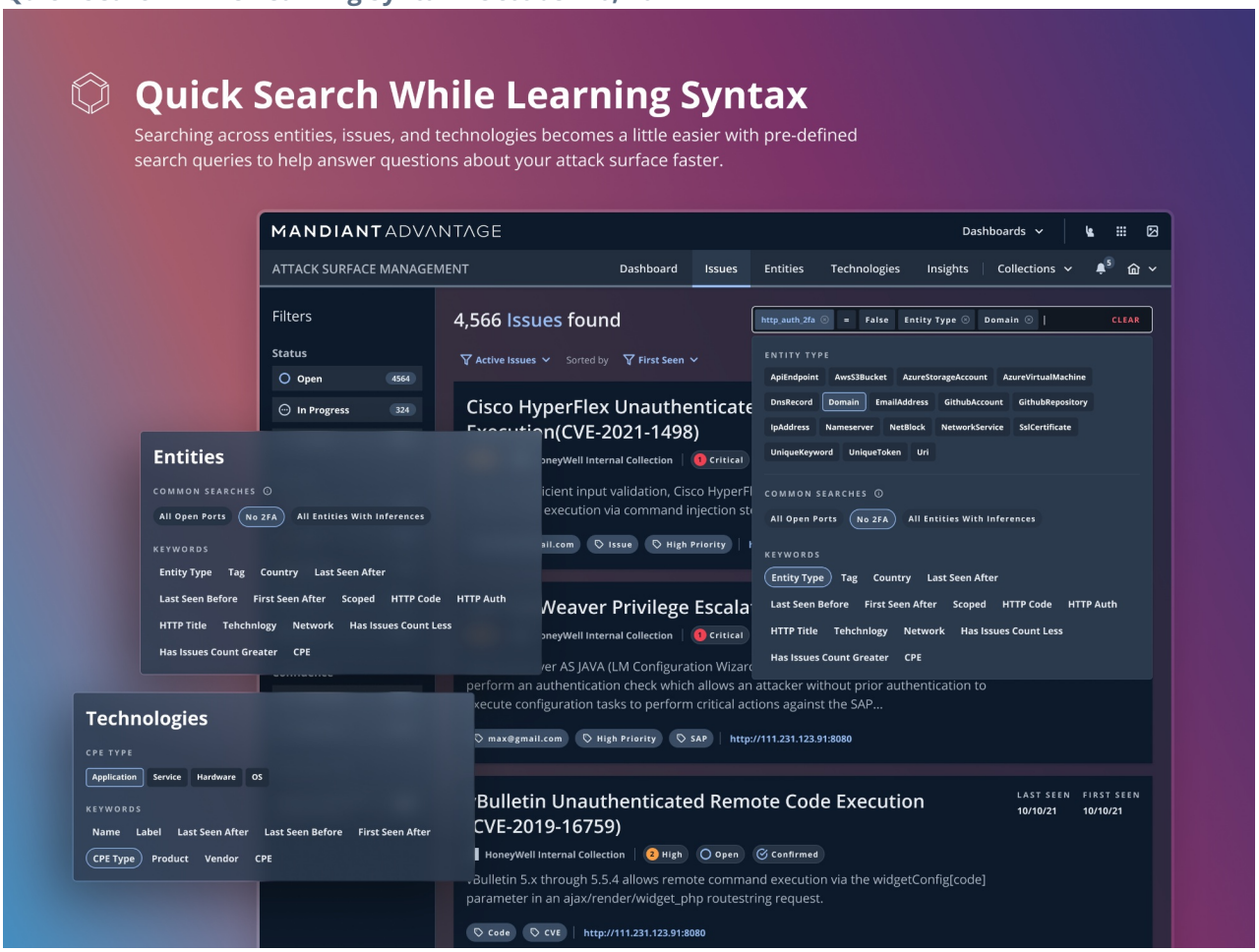
OCTOBER 2022 ASM RELEASES

Quick Search While Learning Syntax - October 20, 2022



Searching across entities, issues, and technologies becomes a little easier with pre-defined search queries to help answer questions about your attack surface faster. Leverage the quick searches available within the search bar to answer your questions while you learn the syntax.

Common Questions

- What are the critical confirmed issues in my attack surface?
- What are the CVEs discovered in my attack surface (potential or confirmed) in the last week?
- Are we running the vulnerable version of the technology with a recently disclosed 0-day?

Manage Remediation with ServiceNow Vulnerability Response - October 13, 2022

The Mandiant Advantage Attack Surface Management App for ServiceNow Vulnerability Response is now available.

Seamless Issue Remediation

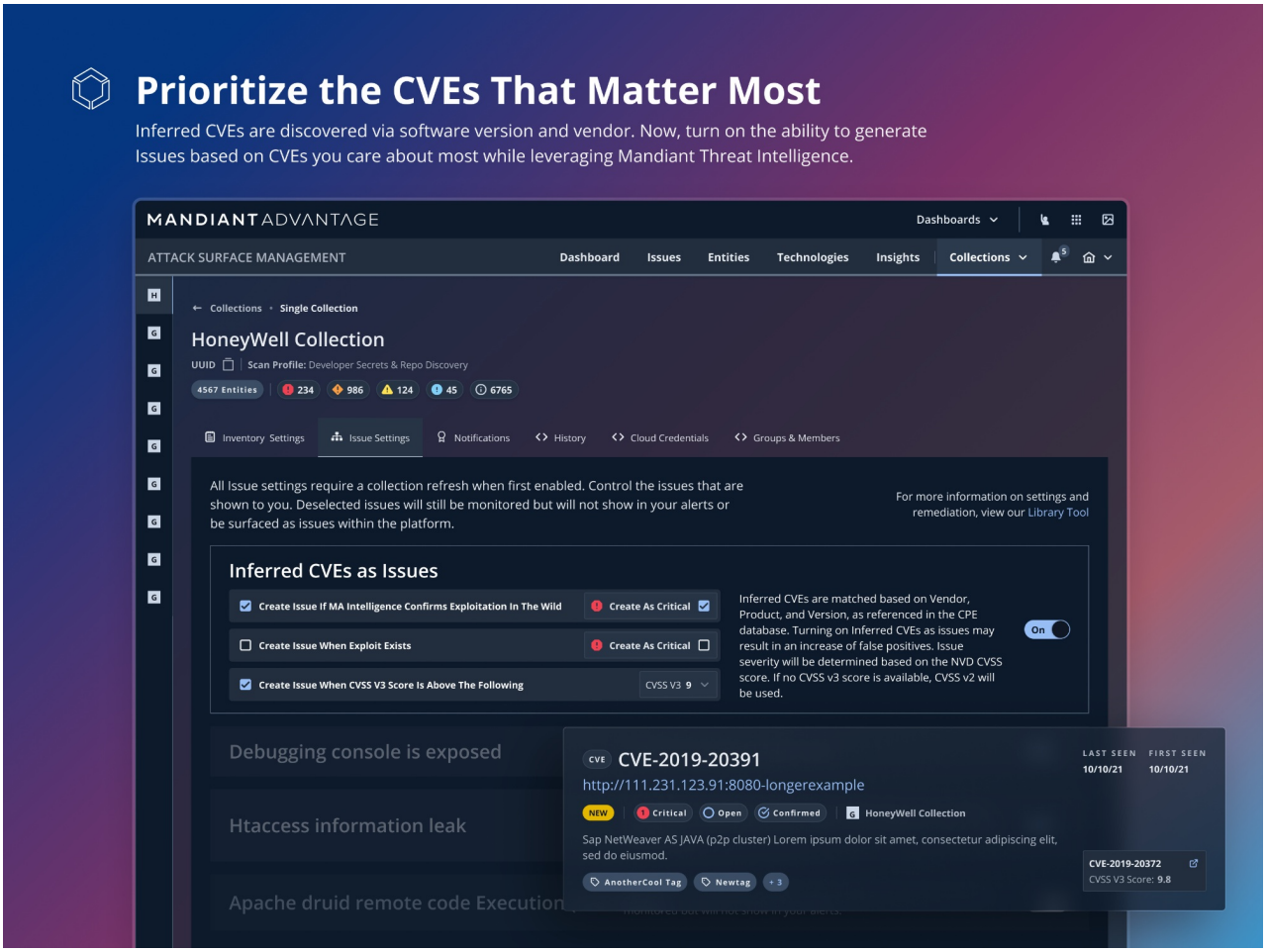
ServiceNow Vulnerability Response uses the ASM API to pull issues into your remediation workflows. The integration allows you to do the following:

- Pull issues from multiple collections within a single project
- Set a minimum severity threshold on the issues presented to the team
- Configure the issue confidence, bringing in potential, confirmed, or both

- Synchronize issue management between ServiceNow and Attack Surface Management; reflect status changes and remediation progress in both products.

Add the App to your ServiceNow instance today (https://store.servicenow.com/sn_appstore_store.do#!/store/application/1ce124b4976951104b4edf14a253aff5/1.0.0).

Prioritize the CVEs That Matter Most - October 11, 2022



Generate Issues from Inferred CVEs

Inferred CVEs are discovered via software version and vendor. Now, turn on the ability to generate Issues based on CVEs you care about most while leveraging Mandiant Threat Intelligence.

Head to **Collection Settings (https://asm.advantage.mandiant.com/collections)** to configure when inferred CVEs generate issues based on the following:

- Active exploitation seen in the wild
- A public exploit code is available
- Align Issue severity to CVSS v3 score

Exchange Server Zero(0)-Day Vulnerabilities - October 3, 2022

Microsoft recently reported two zero-day vulnerabilities (assigned vulnerability IDs: CVE-2022-41040, CVE-2022-41082) affecting Exchange Server 2013/2016/2019. The vulnerabilities require authentication to execute and are unlikely to be leveraged in a mass exploitation event. Furthermore, though an adversary has allegedly leveraged this vulnerability, no

exploit code has been observed in the wild, limiting access and impact. Mandiant has not observed this activity affecting any customer environments at this time.

Mandiant recommends that organizations apply the **Microsoft suggested workarounds** (https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/)to any on-premises Exchange servers publicly exposed to the internet.

Locate the Exchange Servers Publicly Exposed on the Internet

Follow the link to find your **Microsoft Exchange Servers** (https://asm.advantage.mandiant.com/technologies?table_view=false&search_string=last_seen_after%3Alast_refresh%20%22Microsoft%20Exchange%22) or search for "Microsoft Exchange" in the Technologies page search bar.

We are actively monitoring and will provide a check when more details emerge.

Curate Attack Surface Insights with Custom Dashboards - October 3, 2022

We're excited to announce Custom Dashboards, a new way to curate and customize information from the Mandiant Advantage modules.

Within a single dashboard, you can combine insights from Attack Surface Management with relevant data from Threat Intelligence.

Watch a **recorded demo** (https://videos.mandiant.com/watch/Jg9eS8T98TrmKyScWDU5fe?) for more information.