

JULY 2022 ASM RELEASE

Auto-Discover DNS Records - GoDaddy Integration - July 28, 2022

Expand the scope of your Collection by auto-discovering Entities behind GoDaddy.

The new integration continuously ingests DNS records to improve attack surface visibility in situations where the GoDaddy account manages a substantial amount of DNS records.

You can find the new integration [here](https://asm.advantage.mandiant.com/account/settings/project/integrations) (<https://asm.advantage.mandiant.com/account/settings/project/integrations>).

Latest Checks - Atlassian Confluence, WSO2, and More - July 22, 2022

Checks are continuously added to the [Library](https://asm.advantage.mandiant.com/library/issues?search=&field=&value=) (<https://asm.advantage.mandiant.com/library/issues?search=&field=&value=>) to keep our customers informed about the latest vulnerabilities, misconfiguration, and exposures that impact external assets.

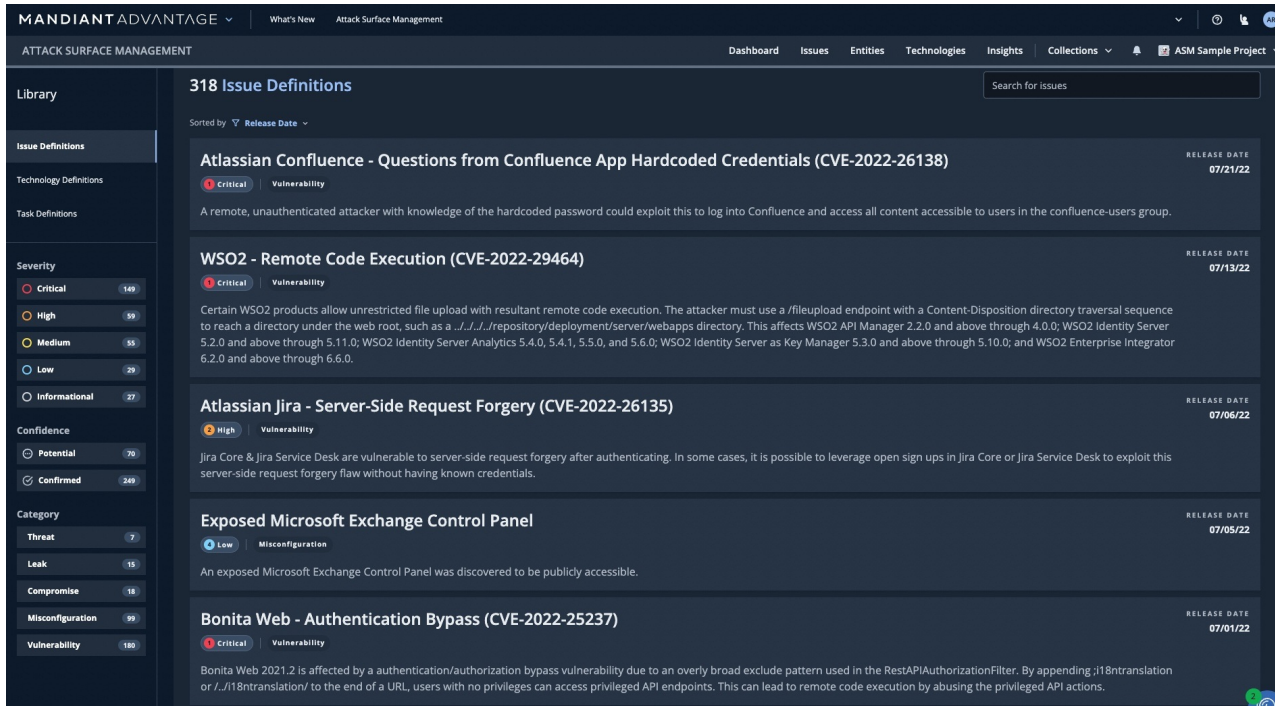
Notable Check:



Atlassian Confluence - Questions from Confluence App Hardcoded Credentials (CVE-2022-26138)

See the latest:

- WSO2 - Remote Code Execution (CVE-2022-29464)
- Atlassian Jira - Server-Side Request Forgery (CVE-2022-26135)
- Exposed Microsoft Exchange Control Panel
- Bonita Web - Authentication Bypass (CVE-2022-25237)



The screenshot displays the Mandiant Advantage ASM interface. The top navigation bar includes 'MANDIANT ADVANTAGE', 'What's New', and 'Attack Surface Management'. The main header shows 'ATTACK SURFACE MANAGEMENT' and a search bar for issues. The left sidebar contains filters for 'Library', 'Issue Definitions', 'Technology Definitions', 'Task Definitions', 'Severity' (Critical: 149, High: 59, Medium: 55, Low: 29, Informational: 27), 'Confidence' (Potential: 70, Confirmed: 249), and 'Category' (Threat: 7, Leak: 15, Compromise: 18, Misconfiguration: 99, Vulnerability: 180). The main content area, titled '318 Issue Definitions', lists several issues:

- Atlassian Confluence - Questions from Confluence App Hardcoded Credentials (CVE-2022-26138)** (Critical, Vulnerability, Release Date: 07/21/22). Description: A remote, unauthenticated attacker with knowledge of the hardcoded password could exploit this to log into Confluence and access all content accessible to users in the confluence-users group.
- WSO2 - Remote Code Execution (CVE-2022-29464)** (Critical, Vulnerability, Release Date: 07/13/22). Description: Certain WSO2 products allow unrestricted file upload with resultant remote code execution. The attacker must use a //fileupload endpoint with a Content-Disposition directory traversal sequence to reach a directory under the web root, such as a .././../repository/deployment/server/webapps directory. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0.
- Atlassian Jira - Server-Side Request Forgery (CVE-2022-26135)** (High, Vulnerability, Release Date: 07/06/22). Description: Jira Core & Jira Service Desk are vulnerable to server-side request forgery after authenticating. In some cases, it is possible to leverage open sign ups in Jira Core or Jira Service Desk to exploit this server-side request forgery flaw without having known credentials.
- Exposed Microsoft Exchange Control Panel** (Low, Misconfiguration, Release Date: 07/05/22). Description: An exposed Microsoft Exchange Control Panel was discovered to be publicly accessible.
- Bonita Web - Authentication Bypass (CVE-2022-25237)** (Critical, Vulnerability, Release Date: 07/01/22). Description: Bonita Web 2021.2 is affected by an authentication/authorization bypass vulnerability due to an overly broad exclude pattern used in the RestAPIAuthorizationFilter. By appending ;!18ntranslation or /!18ntranslation/ to the end of a URL, users with no privileges can access privileged API endpoints. This can lead to remote code execution by abusing the privileged API actions.

Searching for Answers - 2FA Edition - July 15, 2022

Use the search function on the Entities page to answer questions about your external security posture.

1. **What application endpoints in my primary domain don't allow 2FA?**
 - [Check out your application endpoints not protected by 2FA](https://asm.advantage.mandiant.com/entities?) (<https://asm.advantage.mandiant.com/entities?>)

[table_view=false&search_string=%20http_auth_2fa%3Afalse%20last_seen_after%3Alast_refresh](#)). Or,

- Copy & paste **http_auth_2fa:false** in the Entities search bar.

2. What application endpoints in my primary domain allow 2FA?

- **Check out your application endpoints protected by 2FA** (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=%20http_auth_2fa%3Atrue%20last_seen_after%3Alast_refresh). Or,
- Copy & paste **http_auth_2fa:true** in the Entities search bar.

Reporting Insights Beta - July 7, 2022



Our initial round of Reporting Insights has been released for paid customers. Navigate over to the Insights tab to view them.

Reporting Insights Available:

- Top 10 Most Severe Issues
- Top 10 Critical or High Issue Types by Prevalence
- Entities with the Most Issues

You can generate a formatted PDF of this information as well.

New charts and reports will be released on an ongoing basis. We know this is a priority for our customers and will make it a priority for us. All feedback, suggestions, and comments are welcome!

