

## DECEMBER 19, 2025 ASM DISCOVERY ENGINE RELEASE

### Attack Surface Management Discovery Engine release v2025.12.19

This Attack Surface Management Discovery Engine release includes:

#### Bug Fixes

- Added fallback logic for Cymru resolution failures to prevent `net_name` fields from appearing as null.
- Fixed an issue where the Shodan Ranger task could include IPs outside of the range of the netblock.
- Corrected 2FA detection logic in the `enrich/uri` task; previously, `auth.2fa` was incorrectly defaulting to true.

#### Vulnerability Checks

- Adjusted severity for CVE-2025-55182 - React Server Components - Remote Code Execution to reflect its critical nature.
- Added CVE-2025-55183 - Next.js Server Actions - Source Code Disclosure
- Added CVE-2025-59287 - Windows Server WSUS Insecure Deserialization
- Added CVE-2025-66039 - FreePBX Authentication Bypass
- Added CVE-2025-61675 - FreePBX Authenticated SQL Injection
- Added CVE-2025-61678 - FreePBX Authenticated Arbitrary File Upload
- Added CVE-2025-32429 - XWiki Platform - SQL Injection
- Added CVE-2025-55749 - XWiki Platform Information Disclosure
- Added CVE-2025-34299 - Monsta FTP <= 2.11.2 - Unauthenticated Remote Code Execution
- Added CVE-2025-12101 - Citrix ADC/Gateway - Reflected XSS
- Added CVE-2025-8943 - Flowise < 3.0.1 - Remote Command Execution
- Added CVE-2025-6204 - Dassault Systems DELMIA Apriso Command Injection
- Added CVE-2024-20404 - Cisco Finesse Server-Side Request Forgery (SSRF)
- Added CVE-2025-5569 - IdeaCMS <= 1.7 - SQL Injection

#### Technology Fingerprints

- Expanded and consolidated React fingerprints to improve detection of modern Server Component deployments.