Mandiant

SEPTEMBER 25, 2023 ASM DISCOVERY ENGINE RELEASE

Attack Surface Management Discovery Engine release v1.29.0

This Attack Surface Management Discovery Engine release includes:

- **Improved Wordpress Exposed API Issue**
  Reworded the description, added remediation, and added additional references.
- **Improved Exposed Admin Panel Issues**
  Added path in which the fingerprint was discovered to the Issue proof. Created unique Issues for each technology where several fingerprints are discovered.
- **SAP - Memory Pipes Desynchronization (CVE-2022-22536) Active Check temporarily disabled**
  There are active and passive variants of this check. The majority of the findings are passive so the active check has been disabled until it is refactored to work with the new socket helper.
- **Issue reference updates**
  Updated URI reference in description for "Updated Suspicious Web Resource Requested", "Vulnerable Citrix Netscaler (CVE-2019-19781)", "Vulnerable Tomcat - Deserialization in Filestore (CVE-2020-9484)", "Tomcat PersistManager Deserialization RCE (CVE-2020-8494)" and "Jupyter Exposed UI Detection" Issues.

Vulnerability Checks

- **Improved VMWare Workspace One vulnerability check (CVE-2022-22972)**
  Added remediation and tests. Improved check for consistency and reliability of detection.
- **Added Acmailer command injection vulnerability check (CVE-2021-20617)**
- **Added Apache CouchDB vulnerability check (CVE-2022-24706)**
- **Added Tenda AC11 Command Injection vulnerability check (CVE-2021-31755)**
- **Added VMware Aria Operations for Logs remote code execution vulnerability check (CVE-2023-20864)**

Technology Fingerprints

- **Improved fingerprint coverage**
  Added support for compressed responses while fingerprinting technologies via HTTP.
- **Added support for "Configuration Management" technology tag**
- **Improved Tenable fingerprint check**
  Made changes to eliminate false positives when evaluating HTTP response body.
- **Added Puppet technology fingerprints**
  Enables detection of "Puppet" as a vendor, and "Puppet Enterprise", "Puppetboard", "Puppet Dashboard", "PuppetDB" products.
- **Added Pi-Hole technology fingerprints**
  Enables detection of "Pi-Hole" as a vendor/product.
- **Added AVM technology fingerprints**
  Enables detection of "AVM" as a vendor and "FRITZ!Box", "FRITZ!Repeater" as products.
- **Added Shelly IoT technology fingerprints**
  Enables detection of "Shelly" as a vendor, and 1, Plus 1PM, 1 PM, 2.5, EM, Dimmer 2, Pro 1, Duo, 2 Pro, 3EM, PlugS, 4PM as products.
- **Improved Progress MoveIT technology fingerprint**
  Adds cookie-based detection.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.