MAY 30, 2024 ASM DISCOVERY ENGINE RELEASE

Attack Surface Management Discovery Engine release v2024.05.30

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-4040 - CrushFTP - Server-Side Template Injection
- Added CVE-2024-3273 - D-Link Network Attached Storage - Remote Code Execution
- Added CVE-2024-4956 - Sonatype Nexus Repository Manager 3 - Arbitrary File Read
- Added CVE-2024-24919 - Check Point Security Gateway - Arbitrary File Read
- Enhanced multiple Active Checks to identify vulnerabilities accurately, while minimizing the impact on target assets:
  - Adobe Coldfusion Arbitrary Code Execution (CVE-2018-15961)
  - Cisco HyperFlex Unauthenticated Remote Code Execution(CVE-2021-1499)
  - Dynamicweb Logic Flaw Leading to Remote Code Execution (CVE-2022-25369)
  - F5 BIG-IP - Remote Code Execution (CVE-2023-46747)
  - F5 BIG-IP/BIG-IQ - Remote Code Execution (CVE-2021-22986)
  - Fortra FileCatalyst - Remote Code Execution (CVE-2024-25153)
  - Fortinet FortiNAC - Remote Code Execution (CVE-2022-39952)
  - Oracle E-Business Suite - Remote Code Execution (CVE-2022-21587)
  - SAP NetWeaver Privilege Escalation (CVE-2020-6287)
  - SysAid On-Premise - Remote Code Execution (CVE-2023-47246)
  - WSO2 - Remote Code Execution (CVE-2022-29464)
  - Zimbra Collaboration Suite - Remote Code Execution (CVE-2022-37042)

Technology Fingerprints

- Updated metadata for Konica Minolta Multifunction Printer