Version 9.4 Release Notes

The following describe the new features and improvements introduced in RiskVision version 9.4 released on February 26, 2019.

CVSS v3.1 Support

The CVSS v3.0 Score tab in the Vulnerability Details page has been renamed to the CVSS v3 Score tab, with all instances of v3.0 within the tab being changed to v3. In addition, there will be a new CVSS v3 Version field in the tab to show which version of JSON the vulnerability is running.

Vulnerability: CVE-2019-19838

General
CVSS v2.0 Score
Enhanced Score
Risk Score
Identification
More Information
References
Exploits
Risk
Affected Entities
Technologies
Patches
Exceptions
CVSS v3 Score
Threats

▼ CVSS v3 Version

CVSS v3 Version: 3.1

▼ Base Score Metrics v3

Exploitability Metrics
Attack Vector Network
Attack Low Complexity
Privileges None Required
User None Interaction

Scope
Scope Unchanged

Impact Metrics
Confidentiality High
Integrity High
Availability High

▼ Environmental Score Metrics v3

Base Modifiers
Modified Attack Vector N/A
Modified Attack Complexity N/A
Modified Privileges N/A Required
Modified User Interaction N/A

Scope
Modified Scope N/A

Security Requirements
Confidentiality Requirement N/A
Integrity Requirement N/A
Availability Requirement N/A

Impact Metrices
Modified Confidentiality N/A
Modified Integrity N/A
Modified Availability N/A

▼ Temporal Score Metrics v3

Exploit Code Maturity N/A
Remediation Level N/A
Report Confidence N/A

▼ CVSS v3 Score

CVSS v3 Base Score 9.8
Impact Subscore 5.9
Exploitability Subscore 3.9
CVSS Temporal Score N/A
CVSS Environmental Score N/A
Overall Score 9.8

▼ About CVSS

Common Vulnerability Scoring System (CVSS)

ⓘ The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Following are useful links related to CVSS.

National Vulnerability Database https://nvd.nist.gov/cvss/v3-calculator?
CVSS Link vector=CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
National Vulnerability Database Version 3
CVSS Calculator

Version 2

Version 1

Text Input Protections

Additional Cross-Site Scripting (XSS) and poor input validation protections have been applied throughout the RiskVision platform to prevent the execution of malicious scripts that have been entered into input fields.

Direct Access to JasperReports Server

Users can now directly access the standalone JasperReports Server (e.g. http://:8480/jasperserver-pro) via any remote machine. The hostname will vary depending on the user's machine.