

## Version 9.7 Release Notes

The following describes the new features and improvements introduced in RiskVision version 9.7 released on February 2, 2022.

### New System Details Hardware Tab

Entities have a new System Details [Hardware](#) tab that displays all hardware type CPEs that have been attached to the entity. Users can add new or existing technologies to an entity or remove it. This will better represent the technologies deployed on a specific asset, provide better correlation of vulnerabilities for assets, and provide better usability when reporting on vulnerabilities affecting specific technologies.

Computer: High17 ★ Favorites

**Installed hardware**

1-3 of 3

[New](#) [Add](#) [Delete](#) [More Actions...](#)

Filter by [- Show all -](#) [Refresh](#)

| <input type="checkbox"/> | Vendor | Product     | Version | CPE URI                                |
|--------------------------|--------|-------------|---------|--|
| <input type="checkbox"/> | 3com   | 3crwe454g72 | 1.0.2   | cpe:2.3:h:3com:3crwe454g72:1.0.2:***** |
| <input type="checkbox"/> | 3com   | 3crwe454g72 | -       | cpe:2.3:h:3com:3crwe454g72:-:*****     |
| <input type="checkbox"/> | 360    | f5c_router  | -       | cpe:2.3:h:360:f5c_router:-:*****       |

### New Related Risks Tab

Risks now have a [Related Risks](#) tab that allows users to view related risks that have been attached from the risk repository. Users can use this tab to add or remove related risks.

Risk: Viruses, No established controls for mobile computers

**Related Risks**

1-3 of 3

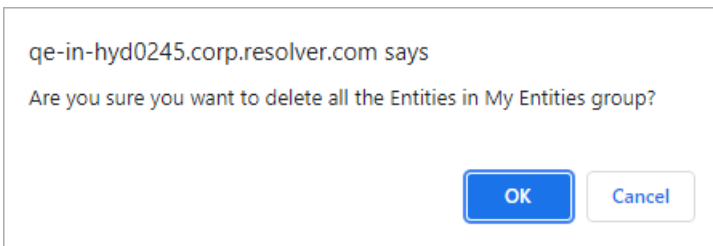
[Add](#) [Remove](#) [More Actions...](#)

Filter by [- Show all -](#) [Refresh](#)

| <input type="checkbox"/> | Title  | Permanent ID | ISO Reference  | Enabled for Assessment | Categories                   | Description  |
|--------------------------|--|--------------|----------------|------------------------|------------------------------|--|
| <input type="checkbox"/> | Application software failure, No logging at application level  | BR0454       | Access Control | Yes                    | Application software failure | Security events are logged at the application level.   |
| <input type="checkbox"/> | DDoS attacks, Disabled Ingress/egress filtering  | BR0390       | Access Control | Yes                    | DDoS attacks                 | Network routers do ingress and egress filtering.   |
| <input type="checkbox"/> | Lawsuits/ litigation, Lack of procedures to verify authenticity of counter party providing electronic instructions | BR0378       | Access Control | Yes                    | Lawsuits/ litigation         | Procedures exist to verify the authenticity of the counter party providing electronic instructions or transactions through trusted exchange of passwords, tokens, or cryptographic keys. |

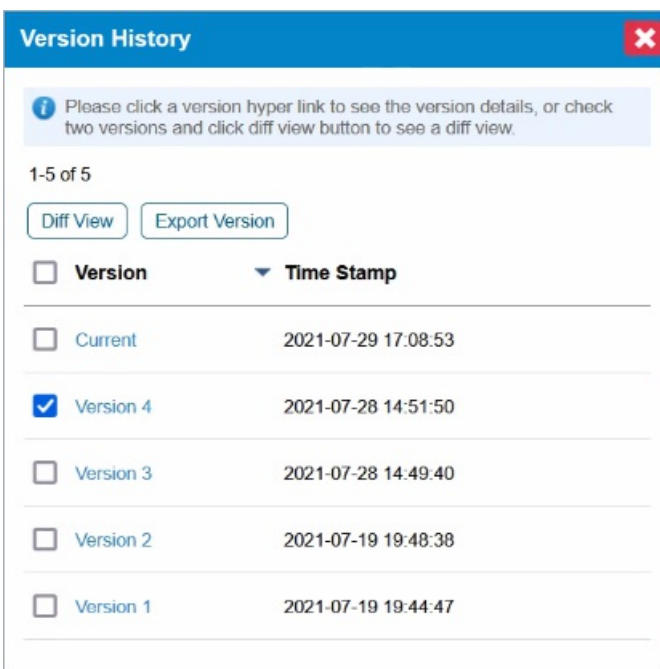
### Improved Entity Deletion Warning

When [deleting an entity](#) with a linked object, a pop-up window will display the name of all linked objects before asking if you wish to continue deleting. When using the Delete All function to delete all entities that are part of a Dynamic Group, a pop-up window will display the name of the Dynamic Group before asking if you wish to continue deleting.



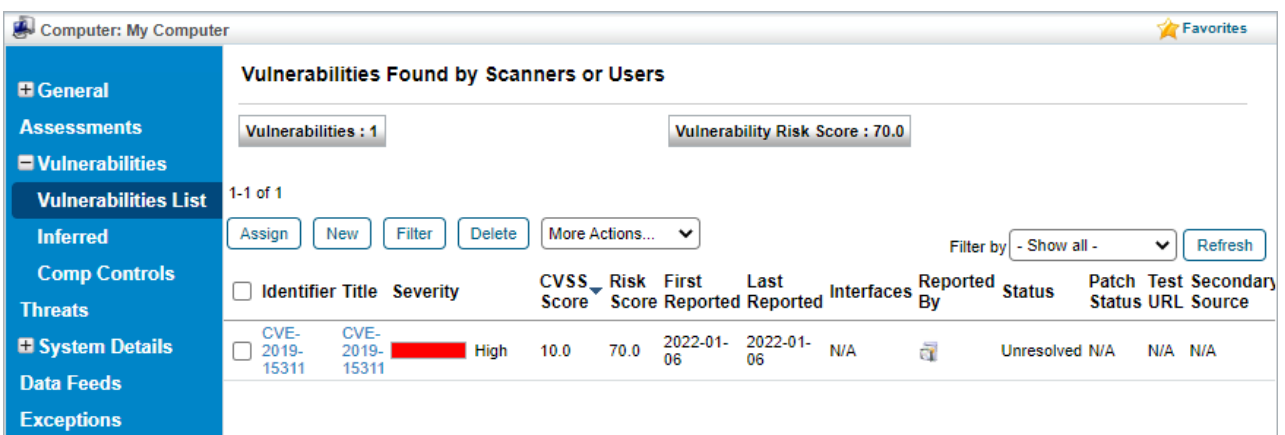
## Export Different Version of Content Pack

Users can now [export](#) different versions of content packs populated with content pack key attributes. This will allow users to view and identify the differences between each content pack version and facilitate more informed decisions for the control going forward.



## New Vulnerability Identifier Column

There is a new Identifier column on an [entity's Vulnerabilities List grid](#) that displays the full identifier code of the vulnerability. The identifier also contains a hyperlink leading to the Vulnerability Instance page.



## CVSS V3.1 Score Calculation

Vulnerabilities that use CVSS V3.1 will now use the 3.1 calculator to calculate their score. If a vulnerability uses CVSS V3.1, the title of the CVSS v3 tab, as well as its score sections, will display version 3.1.

**Vulnerability: CVE-2019-15311**

General

CVSS v2.0 Score

**CVSS v3 Score**

Enhanced Score

Risk Score

Comp Controls

Identification

More Information

References

Risk

Affected Entities

Exploits

Threats

Tickets

Technologies

Patches

Exceptions

**CVSS v3.1 Version**

---

CVSS v3 Version: 3.1

**Base Score Metrics v3.1**

---

|                               |                       |
|-------------------------------|-----------------------|
| <b>Exploitability Metrics</b> | <b>Impact Metrics</b> |
| Attack Vector Network         | Confidentiality High  |
| Attack Complexity Low         | Integrity High        |
| Privileges Required None      | Availability High     |
| User Interaction None         |                       |

**Scope**

Scope Unchanged

**Environmental Score Metrics v3.1**

---

|                                  |                                 |
|----------------------------------|---------------------------------|
| <b>Base Modifiers</b>            | <b>Security Requirements</b>    |
| Modified Attack Vector N/A       | Confidentiality Requirement N/A |
| Modified Attack Complexity N/A   | Integrity Requirement N/A       |
| Modified Privileges Required N/A | Availability Requirement N/A    |
| Modified User Interaction N/A    |                                 |

**Impact Metrics**

Modified Confidentiality N/A

Modified Integrity N/A

Modified Availability N/A

**Temporal Score Metrics v3.1**

---

Exploit Code Maturity N/A

Remediation Level N/A

Report Confidence N/A

**CVSS v3.1 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

## Automatic Of Interest Field Update

Technology assigned to an entity will have the value of its **Of Interest** field automatically changed to **Yes** after the user runs the **Update Technologies Summary** function.

**Technology: Audio File Library Project Audio File Library 0.3.6** Edit

General

References

Vulnerabilities

Entities

Exceptions

**Technology**

---

|   |                                   |
|---|-----------------------------------|
| Full Name Audio File Library Project Audio File Library 0.3.6               | Modified Time 2022-01-20 15:50:26 |
| Description N/A   | Obsolete No                       |
| Vendor audio_file_library_project   | In Use No                         |
| Product audio_file_library  | Banned No                         |
| Version 0.3.6   | Of Interest Yes                   |
| Update *  | Validated Yes                     |
| Edition *   | Part Application                  |
| Language *  |                                   |
| Software *  |                                   |
| Edition   |                                   |
| Target *  |                                   |
| Software  |                                   |
| Target *  |                                   |
| Hardware  |                                   |
| Other *   |                                   |
| CPE URI cpe:2.3:a:audio_file_library_project:audio_file_library:0.3.6:***** |                                   |

## Batch Edit Entity Maximum Size

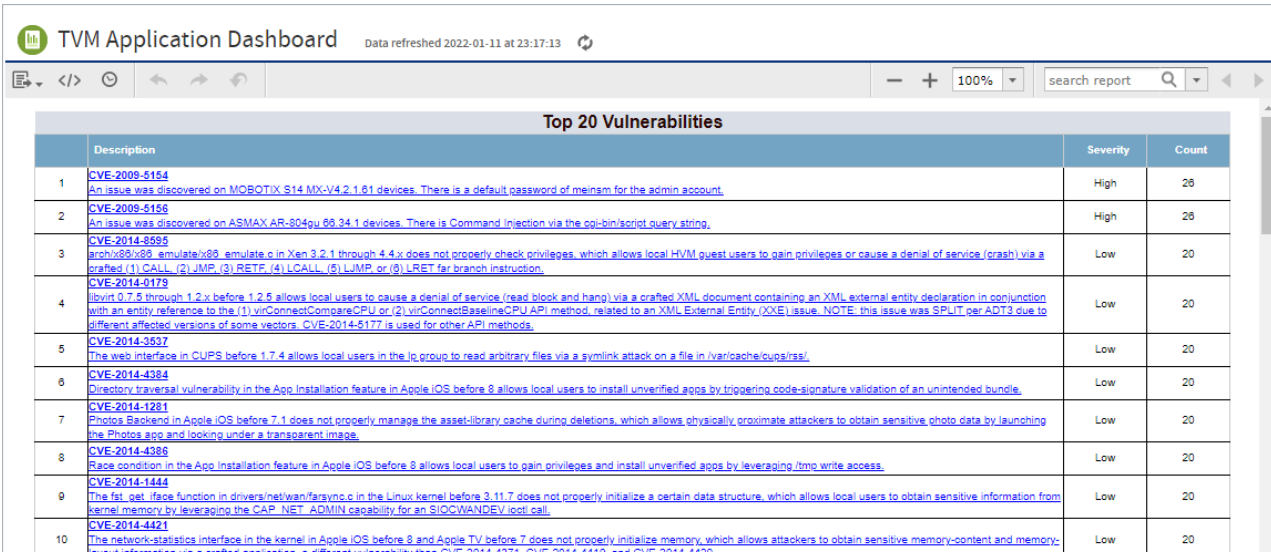
By using the `com.agilience.asset.batchoperations.size` property, users can adjust the maximum size of entities affected by the [Batch Edit Entities](#) action. By default, the maximum size is 50.

## Fix for Apache Log4j 2 Vulnerability

RiskVision has implemented a [fix](#) for a recently discovered vulnerability in Apache Log4j 2 versions 2.0 to 2.17.0. Implementing this fix will make your system less susceptible to Remote Code execution attacks.

## Threat & Vulnerability Manager Dashboard Changes

The [dashboard](#) for the Threat & Vulnerability Manager has been updated to only display the Top 20 Vulnerabilities report. This will free up more resources and prevent application degradation.



The screenshot shows the TVM Application Dashboard interface. At the top, it says 'TVM Application Dashboard' and 'Data refreshed 2022-01-11 at 23:17:13'. Below this is a navigation bar with a search report field. The main content area is titled 'Top 20 Vulnerabilities' and contains a table with the following data:

|    | Description   | Severity | Count |
|----|---|----------|-------|
| 1  | <a href="#">CVE-2009-5154</a><br>An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. There is a default password of meism for the admin account.   | High     | 26    |
| 2  | <a href="#">CVE-2009-5156</a><br>An issue was discovered on ASMAX AR-804pu 66.34.1 devices. There is Command Injection via the cgi-bin/script_query_string.   | High     | 26    |
| 3  | <a href="#">CVE-2014-8595</a><br>arch/x86_64/emulate/x86_emulate.c in Xen 3.2.1 through 4.4.x does not properly check privileges, which allows local HVM guest users to gain privileges or cause a denial of service (crash) via a crafted (1) CALL, (2) JUMP, (3) RETF, (4) LCALL, (5) LJUMP, or (6) LRET far branch instruction.  | Low      | 20    |
| 4  | <a href="#">CVE-2014-0178</a><br>libvirt 0.7.5 through 1.2.x before 1.2.6 allows local users to cause a denial of service (read block and hang) via a crafted XML document containing an XML external entity declaration in conjunction with an entity reference to the (1) virConnectConnectCPU or (2) virConnectBaselineCPU API method, related to an XML External Entity (XXE) issue. NOTE: this issue was SPLIT per ADT3 due to different affected versions of some vectors. CVE-2014-5177 is used for other API methods. | Low      | 20    |
| 5  | <a href="#">CVE-2014-3937</a><br>The web interface in CUPS before 1.7.4 allows local users in the /cups group to read arbitrary files via a symlink attack on a file in /var/cache/cups/ras/.   | Low      | 20    |
| 6  | <a href="#">CVE-2014-4384</a><br>Directory traversal vulnerability in the App Installation feature in Apple iOS before 8 allows local users to install unverified apps by triggering code-signature validation of an unintended bundle.   | Low      | 20    |
| 7  | <a href="#">CVE-2014-1281</a><br>Photos Backend in Apple iOS before 7.1 does not properly manage the asset-library cache during deletions, which allows physically proximate attackers to obtain sensitive photo data by launching the Photos app and looking under a transparent image.  | Low      | 20    |
| 8  | <a href="#">CVE-2014-4388</a><br>Race condition in the App Installation feature in Apple iOS before 8 allows local users to gain privileges and install unverified apps by leveraging /tmp write access.  | Low      | 20    |
| 9  | <a href="#">CVE-2014-1444</a><br>The fst_ops_iface function in drivers/net/wan/farsync.c in the Linux kernel before 3.11.7 does not properly initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability for an SIOCWANDEV ioctl call.  | Low      | 20    |
| 10 | <a href="#">CVE-2014-4421</a><br>The network-statistics interface in the kernel in Apple iOS before 8 and Apple TV before 7 does not properly initialize memory, which allows attackers to obtain sensitive memory content and memory layout information via a crafted application, a different vulnerability than CVE-2014-4371, CVE-2014-4419, and CVE-2014-4420.   | Low      | 20    |

## JasperReports Server 7.9.0

Riskvision can now run up to version [7.9.0](#) of [JasperReports Server](#), delivering the following enhancements:

- Updated User Interface
- Support for new Third-Party Platforms
- New Custom Reports
- JRIO At-Scale
- JasperReports Library Updates