HARMONY
PURPLE

Harmony Purple Release Notes

Release Version: 3.1

Release Date: June 2021

Copyright

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

Contents

New Features and Changes

Release 3.1 of Harmony Purple contains the following new features and changes.

Support of Linux Applications

Harmony Purple now supports the following Linux applications. This support includes scanning for vulnerabilities and recommending remediations.

- 7-Zip
- Adobe Acrobat Reader
- Adobe Flash Player
- Firefox
- Foxit Reader
- Google Chrome
- Gzip
- LibreOffice
- PowerShell
- Thunderbird
- VLC Media Player

Social Vulnerabilities

Research has shown that the most vulnerable point in most information systems is the human user or operator. Social engineering is an increasing security concern.

Social engineering happens because of the human instinct of trust. Cybercriminals have learned that a carefully worded email can convince people to type their credentials into an untrusted website, provide confidential information, open untrusted files sent as attachments, or download a file that installs malware on the company network.

Harmony Purple scans device's applications running on Windows or Linux for social vulnerabilities.

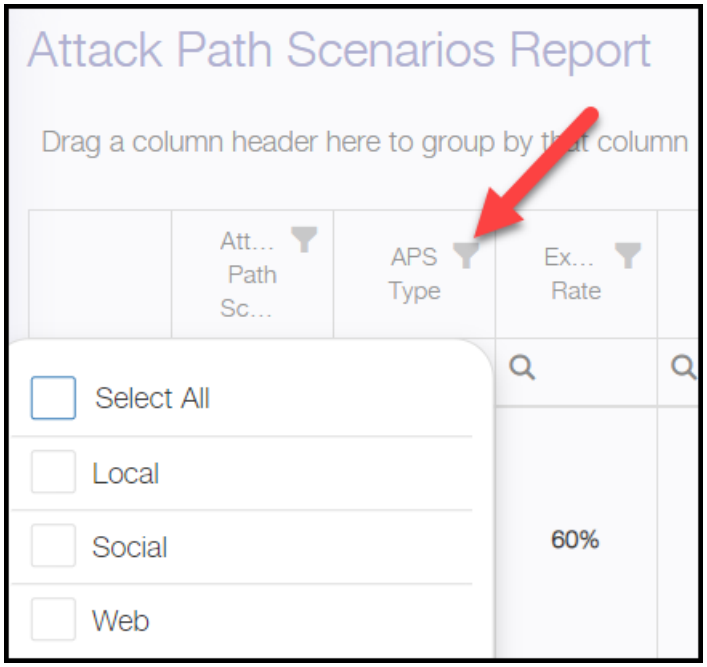
Weekly Content Updates

The weekly content updates now include social vulnerabilities updates.

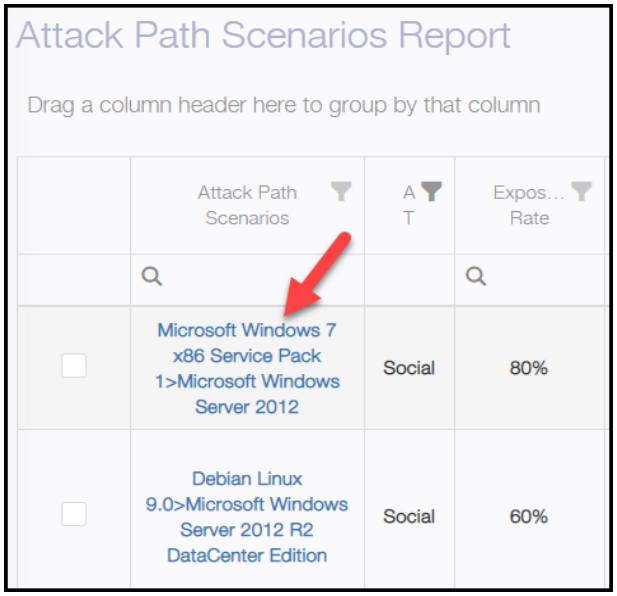
Social Attack Path Scenarios (APS)

There are several changes to the Attack Path Scenarios report.

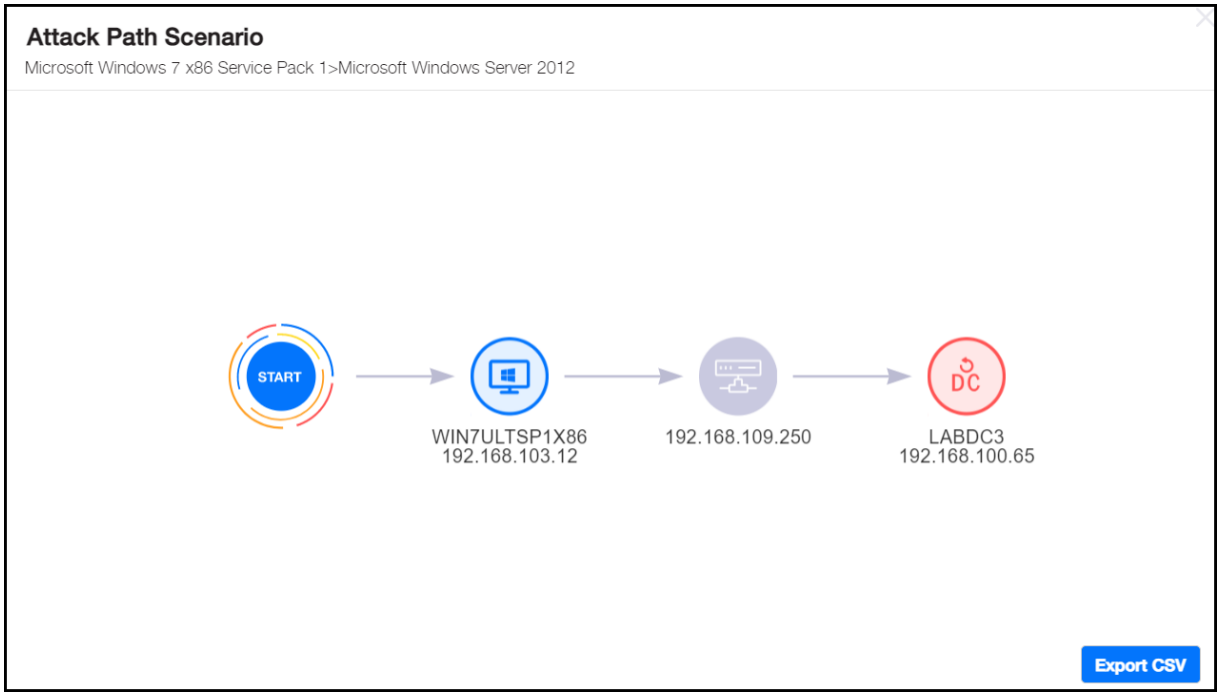
- The APS Type filter has Local, Social (new), and Web (previously called "Global").



- Select the Social Attack Path Scenario's name to view its details.



- The Social Attack Path Scenario displays the path from the starting point device all the way through to the critical asset.

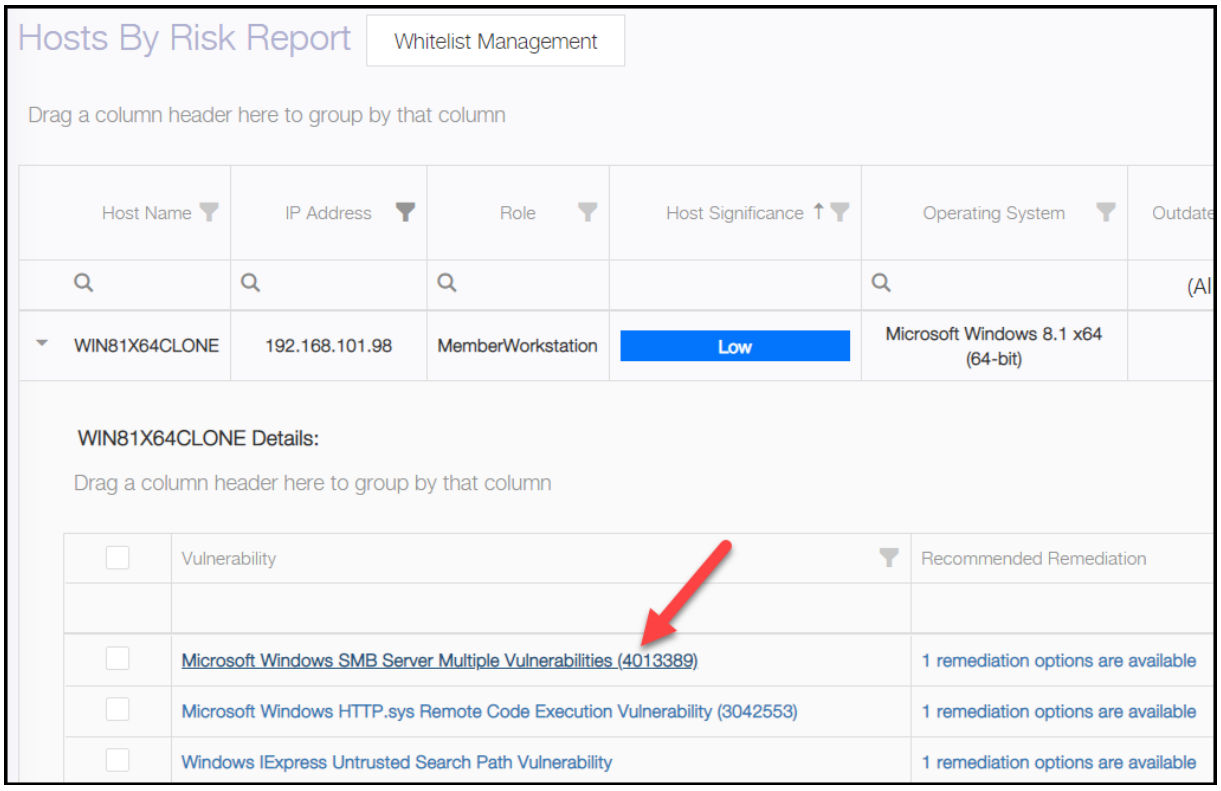


- Select **`Export CSV`** to export the Social APS to a CSV file.
- Hover over any item in the APS to see its details.

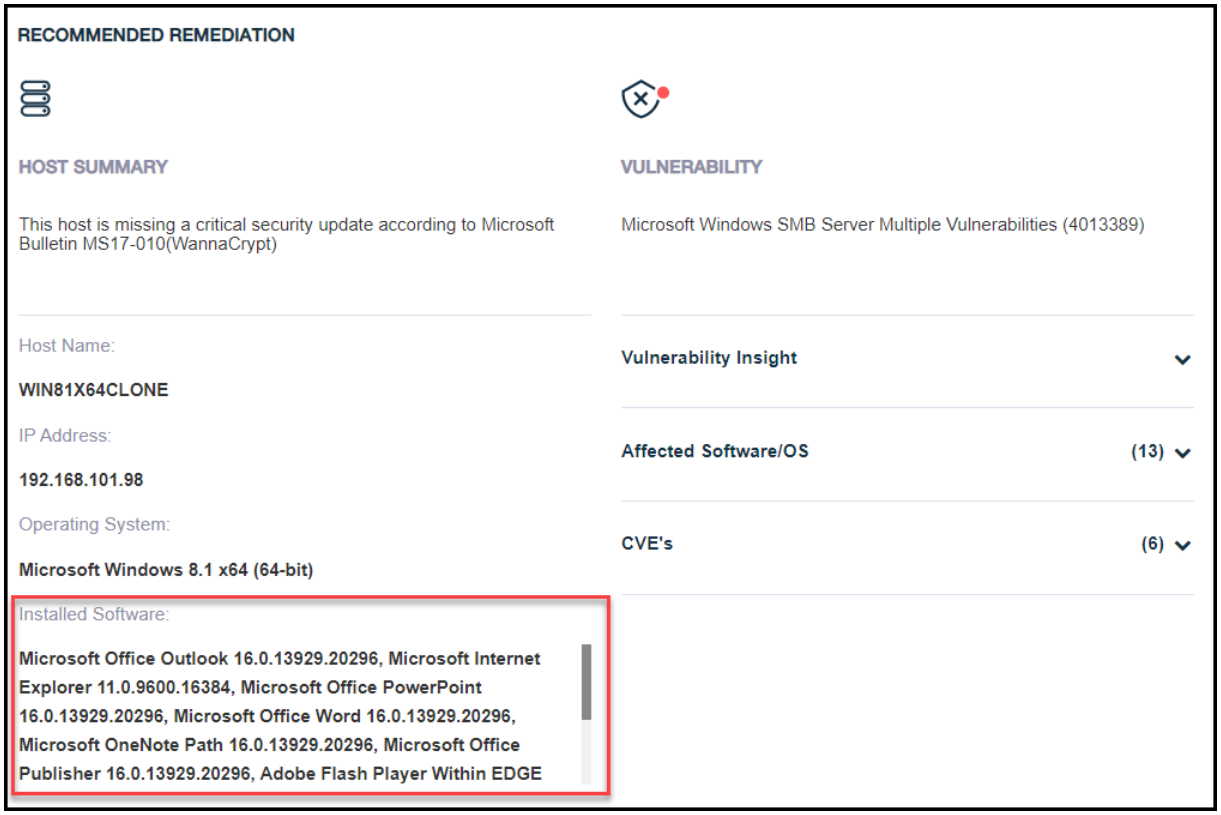
Hosts by Risk Report

The Hosts by Risk report now includes a software inventory of the host.

- Select the Vulnerability.

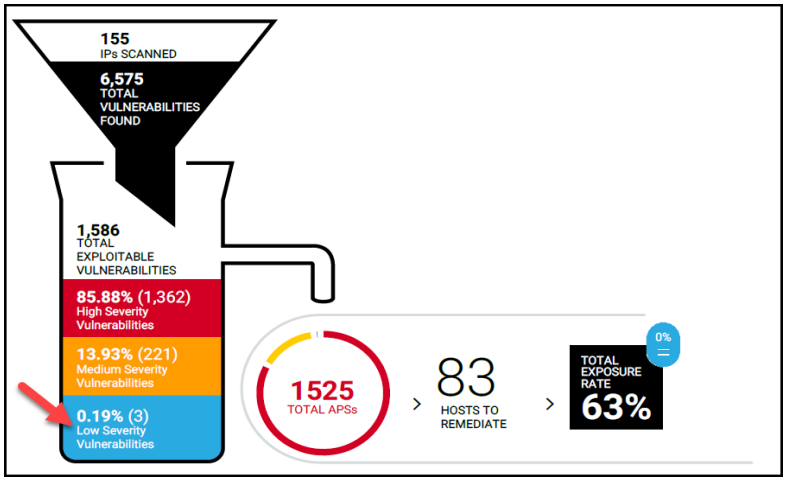


- The Recommended Remediation page now shows a full software inventory of the host.



Executive Summary Report Change

The Low Severity Vulnerabilities in the Scan Summary section of the Executive Summary report now may contain exploitable social vulnerabilities. Previously, Low Severity Vulnerabilities were never exploitable, but some social vulnerabilities, which according to NIST are categorized as low severity, may be exploitable.



Known Limitations

The following limitations are being diligently addressed by our developers.

#	Affected	Description	Internal ID	Reported in Version
1.				
2.				
3.				