



HARMONY  
PURPLE

# Harmony Purple Release Notes

**Release Version: 3.1**

**Release Date: June 2021**

## Copyright

Copyright ©2021 by Orchestra Group Ltd. All Rights Reserved.

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.

No part of this document may be reproduced in any form for any purpose without the prior written permission of Orchestra Group Ltd.

The Orchestra Group Ltd logo and all Orchestra Group Ltd product and service names listed herein are either registered trademarks or trademarks of Orchestra Group Ltd or its subsidiaries. All other marks are the property of their respective owners.

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 .....	4
Support of Linux Applications.....	4
Social Vulnerabilities.....	4
Weekly Content Updates.....	4
Social Attack Path Scenarios (APS).....	5
Hosts by Risk Report.....	7
Executive Summary Report Change.....	8
Known Limitations.....	9

# 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.

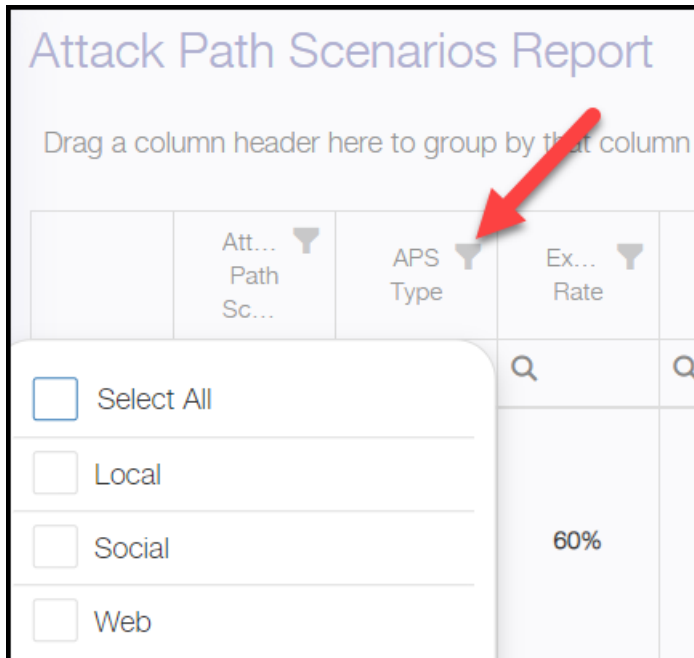
## Weekly Content Updates

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”).

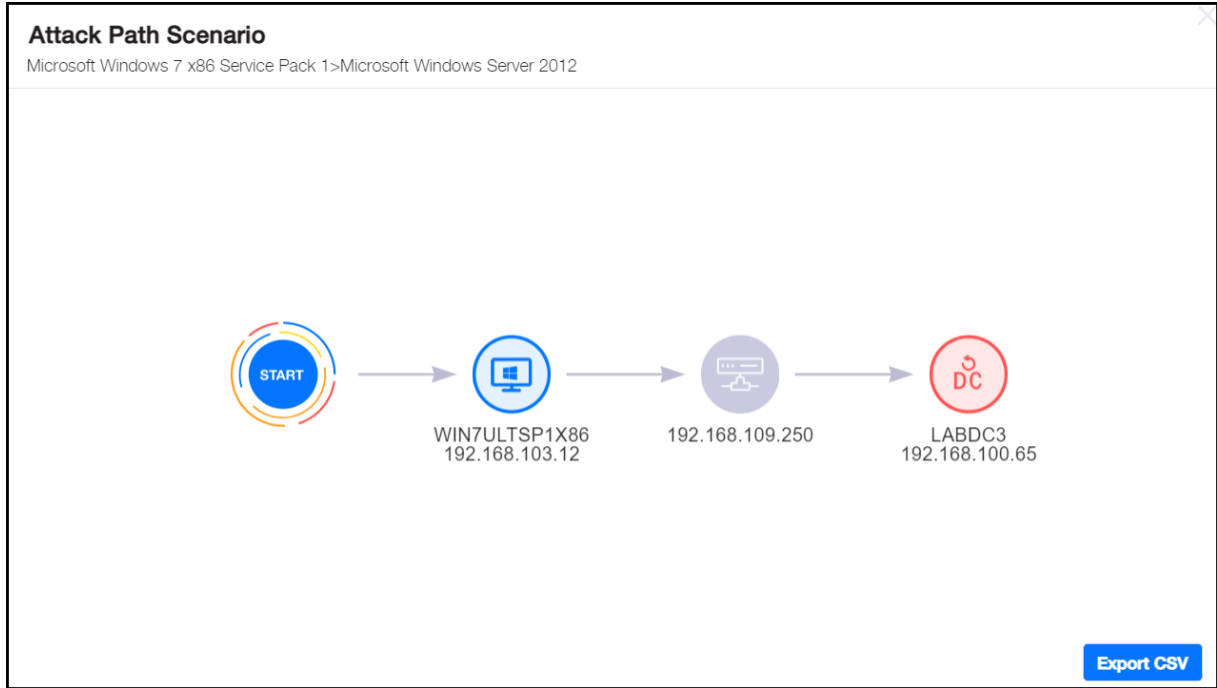


- Select the Social Attack Path Scenario's name to view its details.

The screenshot shows the 'Attack Path Scenarios Report' interface. A red arrow points to the 'Attack Path Scenarios' column header, which has a dropdown arrow. A dropdown menu is open, showing the following options: 'Microsoft Windows 7 x86 Service Pack 1>Microsoft Windows Server 2012' and 'Debian Linux 9.0>Microsoft Windows Server 2012 R2 DataCenter Edition'. The 'Microsoft Windows 7 x86 Service Pack 1>Microsoft Windows Server 2012' option is highlighted. The background shows a table with columns for 'Attack Path Scenarios', 'A T', and 'Exposure Rate'. The 'Exposure Rate' column shows values of 80% and 60%.

	Attack Path Scenarios	A T	Exposure Rate
<input type="checkbox"/>	Microsoft Windows 7 x86 Service Pack 1>Microsoft Windows Server 2012	Social	80%
<input type="checkbox"/>	Debian Linux 9.0>Microsoft Windows Server 2012 R2 DataCenter Edition	Social	60%

- 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.

Microsoft Windows 7 x86 Service Pack 1>Microsoft Windows Server 2012

Host Name:	LABDC3
IP Address:	192.168.100.65
MAC:	00:50:56:9F:26:EF
Role:	BackupDomainController
OS:	Microsoft Windows Server 2012
Vulnerable Port:	53
Vulnerable Service:	dns
Vulnerability:	
	Microsoft Windows DNS Remote Code Execution Vulnerability (3100465)
	Microsoft Windows DNS Server Remote Code Execution Vulnerability (3164065)

## Hosts by Risk Report

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

- Select the Vulnerability.

### Hosts By Risk Report

Whitelist Management

Drag a column header here to group by that column

Host Name ▼	IP Address ▼	Role ▼	Host Significance ↑ ▼	Operating System ▼	Outdate
🔍	🔍	🔍		🔍	(A)
▼ WIN81X64CLONE	192.168.101.98	MemberWorkstation	<b>Low</b>	Microsoft Windows 8.1 x64 (64-bit)	

WIN81X64CLONE Details:

Drag a column header here to group by that column

<input type="checkbox"/>	Vulnerability	Recommended Remediation
<input type="checkbox"/>	<a href="#">Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)</a>	1 remediation options are available
<input type="checkbox"/>	<a href="#">Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (3042553)</a>	1 remediation options are available
<input type="checkbox"/>	<a href="#">Windows IExpress Untrusted Search Path Vulnerability</a>	1 remediation options are available

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

**RECOMMENDED REMEDIATION**

**HOST SUMMARY**

This host is missing a critical security update according to Microsoft Bulletin MS17-010(WannaCrypt)

---

Host Name:  
**WIN81X64CLONE**

IP Address:  
**192.168.101.98**

Operating System:  
**Microsoft Windows 8.1 x64 (64-bit)**

Installed Software:  
Microsoft Office Outlook 16.0.13929.20296, Microsoft Internet Explorer 11.0.9600.16384, Microsoft Office PowerPoint 16.0.13929.20296, Microsoft Office Word 16.0.13929.20296, Microsoft OneNote Path 16.0.13929.20296, Microsoft Office Publisher 16.0.13929.20296, Adobe Flash Player Within EDGE

**VULNERABILITY**

Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)

---

**Vulnerability Insight** ▼

---

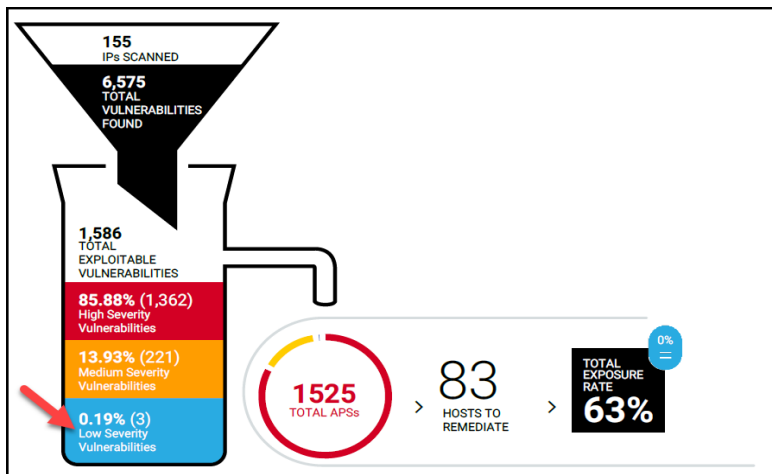
**Affected Software/OS** (13) ▼

---

**CVE's** (6) ▼

## 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.				