LiveAction

LiveWire Omnipeek 25.1.0

Release Notes

What's New In LiveWire Omnipeek 25.1.0

New Features

- Added TACACS+ Groups to Role Based Access Control (RBAC)
- Added more DHCP/DNS Expert Events to Omnipeek
- Improved hardware deduplication
- Added support NPKT format including compression
- Added new TCP Handshake Expert and LiveFlow AVC field
- Added support for the TCPDump Adapter to LiveWire Omnipeek
- Added more items to Engine Configuration Sync
- Added more DHCP/DNS LiveFlow Alerts to LiveFlow

Key Bug Fixes

- Fixed Expert Events in Summary view so they are listed in a logical order.
- Fixed Forensics search on non Napatech captures that are always missing one packet.
- Fixed Protospecs so that RTP payload types in the range 35-63 are accepted.
- Fixed Security Events from displaying wrong data.
- Fixed Liveflow data from displaying incorrect application names.
- Fixed IPMICFG output from displaying wrong management interface.
- Fixed the resize handles in Compass so that they are visible.
- Fixed the Compass background from displaying incorrectly in dark mode.
- Fixed the Forensics view sparkline data after auth token refresh when using multi-engine.
- Fixed that the correct management port is selected on the LiveWire Edge 1515.
- Fixed the active LiveFlow log so it is available in the /var/log/liveflow directory.
- Fixed scrolling with large packet counts.
- Fixed a crash in SMB reassembly.
- Fixed MSA selection display issues.
- Fixed the LiveFlow log file from displaying unreadable binary characters.

Known Issues

- The following Expert events won't work in a monitoring capture when using a Napatech card: TLS Forbidden Version, TLS Slow Handshake, TLS Certificate Invalid Before Date, TLS Certificate Invalid After Date. (OD-4291)
- If a filter was created using an application with version 23.2 or earlier, the filter won't be converted to use new application IDs and will have to be recreated. (OD-3682)
- Those wanting to use RSA SecurID for authentication should choose RADIUS authentication in Omnipeek, and then enable their RSA authentication server's RADIUS option. (OD-2590)
- Filtering when opening a capture file does not work with encrypted files (such as those created by ORA) since Omnipeek has no means of filtering them before they are decrypted and opened. (33175)
- Application classification is done with entire packet contents before slicing is applied when saving packets, so when the file is reloaded the entire packet is no longer present which may result in different (or no) application classification. (30074)
- Application classification may return different results if all the packets that make up a flow are not present, in particular the TCP handshake packets. (30081)
- Cisco and Aruba access points may report incorrect signal and noise percent values in Omnipeek. (29604, 29616)
- In a tcpdump capture, if no packets are filtered and you stop the capture on some remote systems (e.g., Mac OS and Debian Linux), the remote tcpdump processes might not shut down. You may need to SSH into the remote system and shut down the tcpdump processes manually. (29576)
- If the installer launches Omnipeek for you, it is not possible to open a file by double-clicking or 'dragging and dropping' it in Omnipeek. (26149, 26155)

Technical Tips and Additional Product Information

- **Open Source Software**
  This product may include open source software. See the Copyrights folder for more information.

How to Contact LiveAction Online Support

If you can't find the answers that you are looking for in the online help or the User Guide, you can get the most current information from our website. To access the LiveAction website, launch your web browser and go to *https://www.liveaction.com/support/technical-support/*.