TXOne Release note- Firmware

Product type	Industrial EdgeIPS-Pro	Release Date	2021/09/27

1. Release version

- **Firmware name:** ipsp.fw.t01_IPSP_T01_1.2.11.acf
- **Version:** IPSP_T01_1.2.11
- **Revision:** 7753b241
- **SHA256 Checksum:** 2273267de056d3e9340a6ef9b22ad074f21e5c2a12420f4da72dcf5981663ecf
- **Signature info:** TM_IPSP_210910_10
- **CVER:** 1.0.5

2. Applied models

- **Platform: x86_64**
  - IPS-Pro-1048-BP-TM(SE)
  - IPS-Pro-2096-BP-TM

3. Release info

- TOS: ipsp_t01_1.2.11
- Platform (x86_64): ipsp_t01_1.2.11
- Import: ipsp_t01_1.2.11
- TDTS: ics/2.6.18

A. New Features

- [IPS Pattern] Download release notes
- [IPS Pattern] Download rules meta
- [System Page] Add a time series chart of network traffic bandwidth
- [System Page] Add per-port connection status
- [System Page] Add per-port stats
- [Antivirus Pattern] Download release notes
- HA LED turns on when HA is enabled and turns off when HA is disabled.
- [Protocol Filter] Protocol support by signature update
- Streaming Antivirus Detection
- Network visibility enhancement(MAC OUI)
- SNMP modification(SysID)
- Add Mitre ID (TID)
- Bandwidth utilization widget (In/outbound/transmission quality (Session/Packet)
- EdgeIPS/EdgeFire//EdgeIPS Pro client UI (From ODC to Device)
- Default IPS profile
- Viewer access permission change- available for enable packet capture
- meta info download in IPS Rule
- Release note download in the pattern update page
- Support CLI cmd

B. Improvement

- Modify the audit log message of antivirus file exceptions.
- [All][FileExceptions] Change the wording from "Exception Files" to "File Exceptions"
- Add disk info to diag tarball
- Add 'reset asset' command in debug vshell
- Support NVME disk commands in x86_64 platform of debug
- [AVDB] Limit the maximum number of SHA1 records.
- Collect device status periodically
- [Real Time Session Status][Dashboard] Suggest to adjust the circle's size
- [Bandwidth Utilization][Dashboard] Suggest to adjust the location of "0"
- [Syslog] Modify the name of available logs.
- Reorg Asset Search Flow
- [Pacp] Allow viewer to download pcap files
- [Port Security] layout broken

- [Signature Info] Add a new field for mitre techniques
- [System/Audit Log] Modify some messages.
- [Policy Ruleset] Remove Advanced Action
- Port Security – Support batch update
- [Port Status] Change "hwBypassEnabled" to "forceOpen"
- Support more USB disks (Industrial grade vendors: Innodisk and Apacer)

C. Bug Fix

- The Word in Create Policy Enforcement Rule Screen could not be Appropriate
- [IPS][mgmtplane]fatal error: runtime: out of memory
- Hostname could not display successfully.
- When user incorrectly use wrong port and switch back, some asset still appears and won't age out.

D. Known issue

- Win10 SMB client
  - When using Win10 SMB client to connect to a SMB server, just browsing the folder could generate some file filter logs
    - The windows' SMB client will download partial contents of files even if users don't download them
      - [File Filter]Show others file name via SMB protocol
  - When Win 10 SMB client tries to copy a file from SMB server, the client might issue the read request command twice for the same file but with different file Id / uuid
  - When Win 10 SMB client tries to delete a file from SMB server, it will also create file filter log
- [IPS] Cannot apply new rules in default pattern for dataplane to inspect traffic
- After switch standby partition not upgraded partition, if “Management Method” is different from running partition (ex: HTTP, HTTPS) then login page will not be redirect correctly.

E. Software limitation

- According to proprietary protocol and specific setting in the specific OT environment. Possibility EdgeIPS-Pro cannot detect since EdgeIPS-Pro support well known the OT protocol, and only do best effort.
- Policy enforcement cannot block ICMP rules which are based on reversed direction
- Don’t support offline mode of each pair configuration.
- EdgeIPS Pro installation position is close to OT core network and switch port will be one to one connect with EdgeIPS Pro pair and running inline mode. Current version release doesn't support offline mode of each pair.
- The max frame size of IP de-fragmentation is 9000 bytes
- PE malware detection:

  - HTTP
    - Some HTTP clients (e.g. Chrome) can cache partial content for a long time. If resuming download start after 600 sec, IPSP might not block it.

- SMB
  - Out-of-order and SMB3 multi-channel aren't supported
- File filter doesn't support compressed files

- When using FTP protocol to transfer files and TCP FIN flag isn't set in the last packet, Anti-Virus cannot work normally
- File filter limitation

  - HTTP: If the depth of directories is over than 255, filename in log will be shown as 'N/A'

F. Notes

- In current design, when service object to set to 'ICMP' and action is set to 'Deny', it won't work if 'Type/Code' are set as response categories or they are related to the other connection.

Comments :