

TXOne Release Note- Firmware



Product type	Industrial EdgeIPS	Release Date	2020/08/24
1. Release Version <ul style="list-style-type: none">● Firmware Name: ips.fw.g02_IPS_G02_1.1.7.acf● Version: IPS_G02_1.1.7● Revision: ddc71ffe● SHA256 Checksum: 35ad8dd65b21ec53e443b2951feeee9d830d7efb13cee7cc7169eb7b81eb249a● Signature Info: TM_200806_16			
2. Applied Models <ul style="list-style-type: none">● Platform: ARM64<ul style="list-style-type: none">- IPS-102-BP-TM			
3. Release Info <ul style="list-style-type: none">● TOS: ips_g02_1.1.7● Platform (imx8mm): ips_g02_1.1.5● Import: ips_g02_1.1.5● TDTS: ics/2.3.5 A. Support Features <ul style="list-style-type: none">● [New Feature] - Active Query supported in “Visibility Page > Asset View”.● [New Feature] - IPS Profile (Rule Editing) supported in “Object Profiles > IPS Profiles”.● [New Feature] - New OT protocols and options below are supported in “Object Profiles > Protocol Filter Profiles.”<ul style="list-style-type: none">• Added OT protocols support (Basic Settings) - SECS/GEM and IEC61850-MMS• Added OT protocols support (Advanced Settings) - CIP, Siemens S7COMM, Siemens S7COMM PLUS, SLMP, MELSOFT, and TOYOPUC.• Added “Drop Malformed” for strictly packet format checking.• The maximum profile number increases from 16 to 32.● [New Feature] - New options below added in “Security > Policy Enhancement”<ul style="list-style-type: none">• New object types support - IPS profile (New) and protocol filter profiles (New OT Protocols).• Added VLAN support (Up to 5 VLAN ID).• The maximum rule number increases from 64 to 512. B. Improvement <ul style="list-style-type: none">● [Enhancement] - New design of web console.● [Enhancement] - OT protocol monitoring available in offline mode.● [Enhancement] - The maximum capacity concurrent session increases from 10,000 to 30,000.● [Enhancement] - Firmware downgrade feature supported.● [Enhancement] - LEEF log format supported.● [Enhancement] - New log information supported.<ul style="list-style-type: none">• Cyber Security Logs: Interface, Attacker and VLAN ID• Policy Enforcement Logs: VLAN ID• Protocol Filter Logs: VLAN ID and Interface			

- [Enhancement] – Configuration interface of date and time is optimized in “Administration > System Time”.

C. Bug Fix

- [TXN-1763] - [CPU high utilization] After IPS connected to ODC, IPS CPU utilization spikes.
- [TXN-1769] - asset_store has fd leakage

D. Known Issues

- [TXN-1743] - Show maintenance page in short time after upgrade from 1.0.8 to 1.1.5.
- [TXN-1760] - ODC 1.0.x can apply config to IPS devices w/ new 1.1.x FW.
- [TXN-1767] - Command/function category of the OT protocols will get wrong mapping when IPS 1.1 uses the previous pattern of which the version < 200723_15.

E. Software Limitation

- Policy enforcement cannot block ICMP rules based on the reversed direction.
- EdgeIPS doesn't support VLAN QinQ traffic.
- Active Query of assets in inline mode
 - The subnets of MGMT and data MUST be the same.
 - Service ports are fixed for detection: MODBUS (TCP: 502), CIP (TCP: 44818), FINS (TCP: 9600) and SMB (TCP: 445).
 - The queried asset MUST be a server and can send back expected responses to EdgeIPS according to our query commands.

F. Note

- In the current design, when a service object is 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 :