OTU-8000 SmartOTU

Release Notes – 6 May 2021

V20.22 – 6 May 2021

Bugs Fixing

- 8232: shortAcq started on detection/localisation without SmartAcq
- 8246: SmartAcq Not working with DWDM Module

-

V20.16 – 25 Feb 2021

Bugs Fixing

- 8102 : "missing ref trace" on fiber degradation after upgrade to 20.12

V20.12 – 08 Feb 2021

Enhancements

- 7670: Flash Monitoring for Flapping diagnostic

V18.96 – 24 Dec 2020

Bugs Fixing

- 7925: High sensitivity option not available after autotest
- 8012: External switch (OSX) not detected

V18.94 – 18 Nov 2020

Bugs Fixing

- 7740 : False alarm temperature in SmartAcq mode (short + Long pulse) when traffic is amplified
- 7791: Downgrade issue 18.88->18.66

V18.88 – 24 August 2020

No changes for SmartOTU. All changes are for ONMSi V4.50 compatibility

V18.86 – 1 July 2020

Enhancements

- 7451: Support of 144 ports optical switch

Bugs Fixing

- 7646 : blocking after upgrade when alarms are present
- 7656 :: False alarm on reflective fiber end

V18.80 – 1 June 2020

Enhancements

- 7333: SNMP Walk

Bugs Fixing

- 7521: SMTP output syntax issue according to RFC 2046

V18.58 – 4 December 2019

Bugs Fixing

- 7307: Main Led never lights or Flash to indicate Local mode

V18.54 – 31 October 2019

Enhancements

- Dual pulse acquisition reducing the front end dead zone to few meters (1)
- Monitoring algorithm enabling Fiber fault location from few meters after the OTDR up to few meters before the end of fiber. (1)
- Root cause of the fiber fault (Connector or fiber)
- High sensitivity monitoring available with OTDR E81162D and E8115D. A software license is required. Consult Viavi sales or partners.
- Web Services REST Application Program Interface. A software license is required. Consult Viavi sales or partners.
- Number of ports display in SmartOTU monitoring view has increased from 24 to 48 per page

(1): After the upgrade there is a specific process described in the embedded user manual to apply the monitoring algorithm and dual pulse acquisition.

Bugs Fixing

- 7005: Wrong alarm message : attenuation instead of fiber break
- 6784: Fiber break not reported properly if an attenuation is higher than 6 db before the fiber break
- 6746: Alarm severity toggling between critical and major
- 6529: Incorrect localization if no events are superior to thresholds

V7.30

General:

- Email Notification: IP Address is replaced by Host Name if configured in DHCP mode.
- Multimode OTDR is supported

Security

- SSH Vulnerability CVE-2018-15473 – Qualys Level 3

V7.20

Peaks monitoring

- Test scheduling can be disabled
- Display of alarm trace if links have Peaks in alarm
- Improvement of peak shift management

Auto diagnostic

- Auto-diagnostic report available in plain text.

Security

- (Potential) vulnerabilities fixed (level 3) in this software release:

Qualys ID	CVE ID(s)	Brief Definition
370845	CVE-2018-7757	Linux Kernel 'drivers/scsi/libsas/sas_expander.c' Local Denial of Service Vulnerability
370846	CVE-2017-18202	Linux Kernel 'mm/oom_kill.c' Local Denial of Service Vulnerability
370847	CVE-2017-18204	Linux Kernel 'fs/ocfs2/file.c' Local Denial of Service Vulnerability
370849	CVE-2017-7492	Linux Kernel 'net/rds/rdma.c' Denial of Service Vulnerability

V7.12

Main enhancements

- Peaks monitoring (License is required)

Other enhancements

- Simplified Threshold setting

Security

- (Potential) vulnerabilities fixed in this new software release : QID 105728 + QID 38679 + QID 38692.

- “New” Vulnerability fixed in this new release (Apache 2.4.6) : QID 87322 (Patches have been applied to fix this vulnerability but is still in the Qualys scan report as Qualys is not able to detect the patches).

V6.54

- OTDR Trace download using HTTPS
- Multiple SNMP managers
- Home button

Security

- Vulnerability: EOL/Obsolete Software: Apache HTTP Server 2.2.x

V6.44

- Qualys vulnerability QID 370435 fixed.
- Linux kernel / glibc : Elevation of privileges (Stack clash)
-
- Patches have been applied for Linux kernel 3.2 and glibc 2.10
- Note : This vulnerability always appears in Qualys report because it seems that Qualys doesn’t manage that the kernels have been officially patched. (2017 June 29th)

V6.42

- User alias is no longer stored in custom file

V6.30

Security

- Vulnerabilities corrections (curl - See Qualys scan report).

Communication

- Configuration of 100MBPS Full Duplex w/o negociation via script