NO:AP1101-2 V.1

Release Note for VigorAP 1070C

Firmware Version:	5.1.2
Release Type:	Important – Review release notes and upgrade if the changes affect your system stability, performance, or security
Applied Models:	VigorAP 1070C

VigorAP 1070C is a 4T4R simultaneous tri-band 11be BE19000 ceiling mount Access Point with PoE for offering power supply and support 1376Mbps @2.4GHz(b/g/n/ax/BE), 5765Mbps @5GHz (a/n/ax/BE), and 11530Mbps @6GHz (ax/be).

New Features

- Support Access Control List rules based on IP Objects and IP Groups.
- Support the "Allow management from WLAN" option under System Maintenance > Management > Service Control.

Improvement

- Improved: Strengthened Linux kernel security to mitigate CVE-2024-36971, CVE-2024-1086, CVE-2021-22600, CVE-2022-2586, CVE-2022-0492, CVE-2022-0185, CVE-2024-50302, and CVE-2025-38352.
- Improved: Web configuration access control to prevent read-only or restricted accounts from adding, editing, or deleting configuration through unauthorized requests.
- Improved: Updated the 802.11r compatibility note to indicate that some wireless clients may experience connectivity or roaming issues when 802.11r is enabled.
- Improved: Active management sessions are now invalidated when the associated account is deleted, disabled, has its password or TOTP settings changed, or is assigned a different role.
- Improved: Hardened the TR-069 configuration path by writing the ACS server URL and credentials directly to the configuration file, removing a privileged command-injection vector.
- Corrected: An issue where the WPS PIN connection status was not displayed correctly.
- Corrected: An issue where the AP could not be added to AP Management on a DrayOS4 router.
- Corrected: An issue where a CA-signed certificate could not be imported after its CSR was generated on the AP.
- Corrected: An issue where enabling Two-Factor Authentication caused a Web UI login timeout even when the correct verification code was entered.
- Corrected: Issues related to IPv6 AH (Authentication Header) handling (CVE-2026-80844, "DirtyAH6") and PPPoE packet handling (CVE-2026-68121, "PPPoEject").

Known Issue

- DrayTek MFUU can only work through Ethernet port P1.
- The 6GHz client number statistics on web Monitoring > Clients List is not displayed.

Notes

- None.

RD NO: 115_10_20