MOXA

Software Name: WDR-3124A

Version No.	Build Date No./ Release Date	Supported OS	Apply to Models	New Features/Enhancements	Bugs Fixed/Changes	Note
1.2	Build_17112115	N/A	WDR-3124A-EU, WDR-3124A-US WDR-3124A-EU-T, WDR-3124A-US-T	1. [Web] Cookie is generated for each login. 2. [Web] Web server only allows single user access to avoid CSRF (Cross-Site Request Forgery) Vulnerability. 3. [Web] When changing the password, the user is notified to use HTTPS. 4. [Web] Encrypt all password transmisson. 5. [Wireless Search Utility] Encrypt the data between the device and Wireless Search Utility.	Bugs Fixed: 1. [Web UI] Prevent information/file access for none logged in users. 2. [Web] Fixes that browser will re-direct to invalid web page, if the web page is tampered. 3. [Web] Fixes the execution of unwanted Linux commands on UI input pages. 4. [Web] Fixes an invalid URL may crash the UI. 5 . [Utility] Configuring eapUser via remote protocol will cause serviceAgent crash 6. [CISCO Talos: Wireless Search Utility] Fixes that service crash in data encryption in some command. 7. [CISCO Talos: Web] Fixes that nonce are same in the same time produced. 8. [CISCO Talos: Web] Fixes that when the HTTP POST is in an invalid format, the web server may crash. 9. [CISCO Talos: Web] Fixes that when the cookie is NULL with special URL, the web server may crash. 10. The following CVE's are fixed. - CVE-2017-13077 - CVE-2017-13078 - CVE-2017-13080 Changes: 1. Default password changes from "root" to "moxa" 2. [CISCO Talos: Web] Login denied if device detect CSRF (Cross-Site Request Forgery) request.	N/A
1.1	Build_15051314	N/A	WDR-3124A-EU, WDR-3124A-US WDR-3124A-EU-T, WDR-3124A-US-T	N/A	N/A	First Release

Software Name: WDR-3124A

Version No.	Build Date No./ Release Date	Supported OS	Apply to Models	New Features/Enhancements	Bugs Fixed/Changes	Note