

Subject: Critical Firmware Update for HALO 2/3 Devices

- Motorola Solutions designs, develops and deploys our products to prioritize data security and protect the confidentiality, integrity and availability of data. We are committed to providing thorough and timely information when updates to our products are required.
- Critical vulnerabilities have recently been identified in the following products and are expected to become public on or about August 8, 2025:
 - HALO 3C devices running firmware version 2.15.0.13 or lower
 - HALO 2/2C devices running firmware version 2.14.3.0 or lower
- If exploited, these vulnerabilities could allow an attacker to gain unauthorized control over the device, including gaining access to the web interface through brute-force attacks and the installation of malicious or unauthorized firmware. We are not aware of any exploitation in our customers' environments, but immediate steps should be taken to safeguard devices.
- The most effective remediation is to ensure HALO devices are running the latest firmware, firmware Version 2.17.0.2, which addresses these vulnerabilities.
 - **For devices connected to the HALO cloud**, there is no action required. Motorola Solutions will apply the update automatically before August 8.
 - **For devices that are not connected to the HALO cloud**, administrators must download the latest firmware from <https://halodetect.com/firmware-tools/> and install it manually. **For installing firmware on more than one unit at a time**, administrators must download the latest version of the Halo Device Manager (HDM) as well. **Please refer to the HALO Administration Manual for additional information:** <https://halodetect.com/manuals-guides/>
 - **Note:** Once the device is updated to this version, you will not be able to revert to previous firmware versions
- Additionally, firmware version 2.17.0.2 contains support for Amplify Occupancy Sensor, compliance with EU RED requirements as well as support for integration to Raptor Technologies Emergency Management software. Please refer to the HALO Administration Manual for additional information: <https://halodetect.com/manuals-guides/>
- Please be reminded of these cybersecurity best practices:
 - **Keep firmware current:** Ensure HALO devices are running the latest firmware to benefit from the newest functionalities, bug fixes and security updates. Firmware version 2.17.02 addresses the vulnerabilities identified in this notice.
 - **Isolate your network:** Do not operate HALO devices on the same network as public Wi-Fi or other networks accessible to the public.
 - **Use strong passwords:** Enforce the use of strong passwords for HALO devices' web interfaces. We recommend using strong passwords of at least 16 characters.
- For questions or assistance with upgrading HALO firmware, please reference this knowledge article and/or contact Motorola Solutions Technical Support at 866-797-1300.