Updated December 20, 2022

Unified Communications

To our Kodiak, WAVE and BSR customers:

Motorola Solutions is aware of PSIRT advisory FG-IR-22-398 issued by FortiGuard. Motorola Solutions uses Fortinet products in some solutions that we sell and offer as a service, and we take this matter very seriously.

What we know

Based on our current analysis, the following Motorola Solutions Unified Communications products **are not impacted** by the vulnerability:

- WAVE PTX
- Kodiak systems in the US
- Critical Connect
- LMR IMW
- WAVE 5000

We have determined that the following Motorola Solutions Unified Communications products **may be impacted** by the vulnerability :

- WAVE On-Prem systems
- WAVE Lite systems
- BSR systems

What we are doing

For systems managed by Motorola Solutions, we will directly reach out to Motorola Solutions' customers and schedule a time for deploying the patch.

Customer Mitigation Strategy

Customers should consider implementing the mitigation in the PSIRT (to disable the SSL VPN feature on their FortiNet systems) until the patch is deployed.

What you can expect from us

Motorola Solutions will remain diligent in monitoring the situation and keeping our customer informed.

Additional updates regarding this vulnerability will be published on our Motorola Solutions customer notification center. We recommend that you bookmark this page to remain abreast of the most recent information that we have available including any recommended actions relating to Motorola Solutions systems, products and software.

Protecting Your Systems - General Guidance

As a general practice, we strongly recommend that Motorola Solutions customers regularly take the following steps to protect their systems:

1. Use only supported configurations in Motorola Solutions products.
2. Apply all updates provided by Motorola Solutions and other vendors as soon as possible.
3. Review user and administrative accounts to ensure no unauthorized accounts are present.
4. When possible, do not allow internet exposure for mission-critical devices and/or systems; when internet exposure is required, always apply strong security controls.
5. Monitor FortiGuard PSIRT advisories and the DHS Cybersecurity & Infrastructure Security Agency's (CISA) vulnerability note.

We are committed to providing secure products and secure services that help people be the best in the moments that matter. Customers who would like more support with this, or any cybersecurity issue, should contact their Customer Support Manager or Account Executive.