December 20, 2022

Two-Way Radio Solutions

To our Two-Way Radio Solutions customers:

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

What we know

Based on our analysis, we know that some instances of our Two-Way Radio Solutions are deployed using a Fortinet SSL VPN to connect remote console positions to the core and for remote system management services. In these cases those Fortinet devices may be vulnerable to the flaw.

What we are doing

We have conducted a thorough analysis to determine exposure and mitigate the risk. The Public Safety Threat Alliance, a Motorola Solutions-led information sharing and analysis organization, continues to monitor the potential impact of this vulnerability to public safety, and our Security Operations Center has implemented detective controls to monitor for any indicators of compromise in customers that we provide with security monitoring. Additionally, our solutions that are offered as a service are actively working to apply mitigations to keep you safe.

What you can expect from us

Motorola Solutions will remain diligent in monitoring the situation and keeping our customers 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

If there is a SSL-VPN on the Fortinet firewall in your deployment, we recommend to immediately patch these firewalls with the Fortinet defined updated FortiOS versions.

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.