Updated December 20, 2022

NG9-1-1 Call Management

To our emergency call management 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 emergency call management products **are not impacted** by the vulnerability:

- CommandCentral Call Handling
- CallWorks

We have determined that the following Motorola Solutions emergency call management products **are impacted** by the vulnerability:

- VESTA Router
- VESTA 9-1-1

What we are doing

- VESTA Router: Security updates have been successfully applied for all customers and no further action is required.
- VESTA 9-1-1: We will directly contact all customers with a Managed Service Monitoring and Response contract to schedule a time for us to apply the security updates. All channel partners will also receive a Technical Service Bulletin to give a green light to apply patches to the systems they manage.

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 - 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.