PSTA
Public Safety Threat Alliance
Public Safety ISAO

Threat Advisory

TLP:GREEN

Threat actor impersonating Motorola Solutions employee

Disclosure Protocol: GREEN: Restricted to the community
Date of Publication: 09 January 2026

Summary

Motorola Solutions recently became aware of a threat actor attempting to gain access to public safety agencies' networks by impersonating a Motorola Solutions support technician. A small number of agencies across the United States have reported receiving phone calls from an individual claiming to work for Motorola Solutions. In each instance that we are aware of, the individual(s) sought authorization to remotely connect to the agency's network to purportedly push a necessary security patch.

In at least one instance, the threat actor specifically referenced products from Motorola Solutions, demonstrating an awareness of mission-critical systems. It is possible the threat actor is mentioning other products and brands relevant to targeted agencies.

We believe the threat actor may continue the campaign against other public safety organizations and encourage our members to remain vigilant.

Please be aware of potential vishing (voice phishing) attacks. When in doubt about the authenticity of a communication, contact a known Motorola Solutions representative directly to confirm an individual's credentials.

Further reading

1. https://www.proofpoint.com/us/threat-reference/vishing
2. https://attack.mitre.org/techniques/T1598/004/

Appendix A: Defense mitigations

Public safety agencies are advised to follow standard best practices to prevent successful vishing attacks:

- ☐ **Verify caller credentials.** If a caller requests sensitive information or access to defender resources such as computers or servers, end the call and contact the associated institution directly using a valid, known phone number or email.
- ☐ **Ignore pressure tactics.** Many phishing and vishing attacks attempt to foster a sense of urgency to make defenders act without thinking. Watch for requests for immediate action, even those related to purported important security measures.
- ☐ **Register with 'Do Not Call' lists.** National 'Do Not Call' registries can help reduce unsolicited calls, reducing the risk of possible scams.
- ☐ **Employ multi-factor authentication (MFA).** Threat actors attempting to log into defender environments should be met with MFA prompts, reducing the effectiveness of stolen or compromised login credentials.
- ☐ **Watch for deepfakes.** Know that AI can be used to mimic some voices, and can allow threat actors to appear more legitimate than they would otherwise. Always independently verify the identity of callers with source organizations.

Appendix B: Assessment and Response Standard Operating Procedures

Levels of Analytic Confidence

High Confidence	Moderate Confidence	Low Confidence
Generally indicates judgments based on high-quality information, and/or the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and still carries a risk of being wrong.	Generally means credibly sourced and plausible information, but not of sufficient quality or corroboration to warrant a higher level of confidence.	Generally means questionable or implausible information was used, the information is too fragmented or poorly corroborated to make solid analytic inferences, or significant concerns or problems with sources existed.

Appendix C: Traffic Light Protocol for Disclosure

As part of the PSTA, agencies and other members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light Protocol (TLP), based upon the CISA Traffic Light Protocol guidance, which helps all members submit and leverage insights while being respectful of the submitting agency's preferences.

RED: Restricted to the immediate PSTA participants only

- When should it be used? Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.
- How may it be shared? Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

GREEN: Restricted to the community

- When should it be used? Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
- How may it be shared? Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

AMBER: Restricted to participants' organizations

- When should it be used? Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
- How may it be shared? Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. TLP:AMBER+STRICT Restricts sharing to the organization only.

CLEAR: Disclosure is not limited

- When should it be used? Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- How may it be shared? Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.