PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov
TTY: 888-835-5322

DA 25-996
Released: November 26, 2025

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU REMINDS BROADCASTERS TO ENSURE THEY COMPLY WITH BEST PRACTICES TO PREVENT CYBERATTACKS

The Public Safety and Homeland Security Bureau (Bureau) of the Federal Communications Commission (Commission) reminds broadcasters of their responsibility to ensure the security of their broadcast networks and systems. In particular, this Public Notice is issued in response to the recent string of cyber intrusions against various radio broadcasters that resulted in the broadcast of obscene materials and the misuse of the Emergency Alert System (EAS) Attention Signal (Attention Signal).[1]

It appears that these recent hacks were caused by a compromised studio-transmitter link (STL)—the broadcast equipment that carries program content from the studio to remote transmitters—with threat actors often accessing improperly secured Barix equipment and reconfiguring it to receive attacker-controlled audio in lieu of station programming. Affected stations broadcast to the public an attacker-inserted audio stream that includes an actual or simulated Attention Signal and EAS alert tones, as well as obscene language, and other inappropriate material.

We urge all broadcasters, especially those using Barix equipment, to:

- Install software security patches issued by the equipment manufacturer as soon as they become available, and upgrade equipment firmware and software to the most recent versions recommended by the manufacturer.
- Change their devices' default passwords and replace them with robust alternatives, and regularly change passwords to promote continued security.
- Where reasonably feasible, install EAS, Barix, and other equipment interconnected to the broadcast signal processing system behind network firewalls, and utilize VPNs that are configured to limit remote management access to only authorized devices.
- Continually monitor EAS equipment and software and review audit logs to detect and report incidents of unauthorized access.
- Review the list of recommended best practices to address potential data security vulnerabilities issued by the Communications Security, Reliability, and Interoperability Council in 2014.[2]

---

[1] *See, e.g.*, Lance Venta, *ESPN 97.5 Houston Victim of Barix Hack* (Nov. 23, 2025), https://radioinsight.com/headlines/321936/espn-97-5-houston-victim-of-barix-hack/; Katelyn Harlow, *NPR affiliate's backup audio signal hacked, 'offensive material' broadcast in Richmond* (Nov. 21, 2025), https://www.wric.com/news/local-news/npr-affiliates-backup-audio-signal-hacked-offensive-material-broadcast-in-richmond-area/.

[2] Communications Security, Reliability and Interoperability Council IV, Initial Report, EAS Security Subcomm. Report at 10-13 (2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG3-EAS_SECURITY_INITIAL_REPORT_062014.pdf.

We encourage broadcasters to contact their EAS equipment manufacturers with any specific questions regarding the security of EAS equipment. If you suspect that broadcast equipment has been subject to attempts at unauthorized access, we recommend you contact the equipment manufacturer and/or a data security firm. We strongly encourage broadcasters who suspect unlawful access to their systems to notify the FCC Operations Center at 202-418-1122 or FCCOPCenter@fcc.gov and to report any cyberattacks to Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) at https://www.ic3.gov/.

Media inquiries should be directed to 202-418-0500 or MediaRelations@fcc.gov.

- FCC -