NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

NCCIC/ICS-CERT ALERT

ICS-ALERT-14-157-01P SITUATIONAL AWARENESS ALERT FOR ELECTRONIC HIGHWAY SIGNS

June 06, 2014

ALERT

SUMMARY

NCCIC/ICS-CERT received reporting from the Federal Highway Administration (FHWA) on June 3, 2014, that multiple states were victims of exploitation of the Dynamic Message Signs (DMS) operated by states' Department of Transportation (DOT).

These signs provide motorists with information related to road conditions, travel times, Amber Alerts, and other important messages. Exploitation of these vulnerabilities could result in inaccurate messaging, derogatory text, improper routing, or possible equipment malfunction indicators.

ICS-CERT is aware of three states confirming compromises of the signs and news reports on the incidents. ICS-CERT is issuing this alert to provide notice of the reports and identify baseline mitigations for reducing risks to these and similar cybersecurity attacks.

ICS-CERT is working with the sign vendor, the security researcher, and a wireless communications vendor that appear to be the access point for the exploitation. At this time, there is no evidence that DOT systems or networks were affected but rather the communication links to the signs themselves.

There is sufficient public information at this time to exploit these vulnerabilities.

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

RECOMMENDED MITIGATIONS

Multi-State Information and Analysis Center's (MS-ISAC), Center for Internet Security suggests implementing the following recommendations for all remote and local DOT equipment, including roadway cameras and traffic signals.

- Use strong, complex passwords on all electronic road signs.
- Change all Simple Network Management Protocol (SNMP) community strings from the default (typically Public or Private) upon receiving the equipment.
- Disable the web interface and telnet functionality. Close all open ports, where possible.
- If SNMP is not used, disable it. If it is used, consider disabling the RW (Read-Write) password for SNMP. If not possible, ensure it uses a strong, complex password, different from the RO (Read-Only) password.
- If possible, use SNMP management stations so changes may only be made from predefined addresses.
- If possible, upgrade to the most current version of SNMP (currently Version 3).
- If possible, place all road signs on a secured wide area network.
- If possible, enable remote logging of all changes and monitor the logs.
- As many sign defacements appear to be the work of local actors, ensure control panels are secured with a strong lock and access to the programming functionality requires the use of a strong, complex password.

For details, please see the MS-ISAC announcement:

http://msisac.cisecurity.org/daily-tips/malicious-cyber-actor-targeting-electronic-road-signs.cfm

Daktronics has the following recommendations:

- Change the default password after receiving new or transferred equipment.
- Ensure displays are not on publically accessible IP addresses. Placing a display on a private network or Virtual Private Networks (VPNs) helps mitigate the lack of security with National Transportation Communications for Intelligent Transportation System Protocol (NTCIP). If this cannot be accomplished, disable the telnet, web page, and web LCD interfaces.
- Use Event Logging. NTCIP defines a method for logging events that is capable on the controller. Log message activations to determine activation of a message from the central control software rather than a local activation (physical pressing buttons on the controller, using the web interface, or using the web LCD interface).

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Disable telnet Port 23/TCP, if applicable.
- Minimize network exposure for all DMS system devices and/or systems and ensure that they are not accessible from the Internet.a
- Locate DMS system networks and devices behind firewalls, isolating them from the business network.
- When remote access is required, use secure methods, such as VPNs, recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also, recognize that VPN is only as secure as the connected devices.

ICS-CERT is currently coordinating with the vendor and security researcher to identify mitigations.

Affected Vendor Notifications:

ICS-ALERT-14-155-01A – Daktronics Vanguard

http://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-155-01A

ICSA-14-007-01A – Sierra Wireless AirLink

http://ics-cert.us-cert.gov/advisories/ICSA-14-007-01A

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT also provides a recommended practices section for control systems on the ICS-CERT web site (http://ics-cert.us-cert.gov). Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

a. ICS-CERT ALERT, http://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01, web site last accessed June 6, 2014.

NCCIC
NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

ICS-CERT Operations Center
Toll Free: 1-877-776-7585
International: 1-208-526-0900
Email: ics-cert@hq.dhs.gov

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov/

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://www.us-cert.gov/forms/feedback.

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.