ICS-CERT ADVISORY

ICSA-12-335-01—POST OAK BLUETOOTH TRAFFIC SYSTEMS INSUFFICIENT ENTROPY VULNERABILITY

November 30, 2012

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts Post Oak Traffic AWAM Bluetooth Reader Systems. An independent research group composed of Nadia Heninger,[a] Zakir Durumeric,[b] Eric Wustrow,[b] and J. Alex Halderman[b] identified an insufficient entropy vulnerability[c] in authentication key generation in Post Oak's AWAM Bluetooth Reader Traffic System. By impersonating the device, an attacker can obtain the credentials of administrative users and potentially perform a Man-in-the-Middle (MitM) attack. Post Oak has validated the vulnerability and produced an updated firmware version that mitigates the vulnerability. According to Post Oak, products are deployed in the transportation sector, mainly in the United States.

This vulnerability can be exploited remotely.

AFFECTED PRODUCTS

The following Post Oak products are affected:

- AWAM Bluetooth Reader Traffic System, all versions.

IMPACT

An attacker can gain unauthorized access to the system by determining the authentication keys from reused or nonunique host keys. By exploiting this vulnerability, the attacker can perform a MitM attack to affect the availability of the system and access data and settings.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

a. University of California at San Diego

b. University of Michigan

c. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices, https://factorable net/paper.html, Web site last accessed November 30, 2012.

BACKGROUND

Post Oak Traffic Systems is a US-based company that specializes in low cost traffic monitoring in both freeway and arterial environments. Post Oak uses licensed patent pending technology developed by the Texas A&M Transportation Institute, a transportation research organization.

The affected products are Bluetooth wireless traffic monitoring systems. According to Post Oak, the product is deployed in the transportation sector. Post Oak estimates that these products are used primarily in the United States.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSUFFICIENT ENTROPY[d]

The Post Oak AWAM Bluetooth Reader Traffic Systems does not use sufficient entropy when generating authentication and host keys. By calculating the private authentication keys, an attacker could perform a MitM attack on the system by knowing the nonunique host key. This could allow the attacker to gain unauthorized access to the system and read information on the device, as well as inject data compromising the integrity of the data.

CVE-2012-4687[e] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[f]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

d. CWE, http://cwe mitre.org/data/definitions/331.html, CWE-331: Insufficient Entropy, Web site last accessed November 30, 2012.

e. NVD, http://web nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4687, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:H/Au:N/C:C/I:C/A:C), Web site last accessed November 30, 2012.

DIFFICULTY

An attacker with a high skill would be able to exploit these vulnerabilities.

MITIGATION

Post Oak has developed a patch for the AWAM Bluetooth Reader Traffic System that mitigates the vulnerability. The patch allows the Bluetooth reader to ensure sufficient entropy exists before generating host and authentication keys. The patch will be installed on all new devices when initially configured. Existing equipment will be patched by remote access and upgraded to the latest firmware. System owners are encouraged to contact[g] Post Oak Traffic Systems with questions patching their systems.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[h] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01—Cyber Intrusion Mitigation Strategies,[i] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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

g. Post Oak Traffic Systems, support@postoaktraffic.com, (281) 381-2887.

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed November 30, 2012.

i. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed November 30, 2012.

ICS-CERT CONTACT

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

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585

For industrial control systems security information and incident reporting: www.ics-cert.org

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://forms.us-cert.gov/ncsd-feedback/.

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events 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.