



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-297-01—TROPOS WIRELESS MESH ROUTERS INSUFFICIENT ENTROPY VULNERABILITY

December 10, 2012

OVERVIEW

This advisory is a follow-up to the original advisory titled ICSA-12-297-01P—Tropos Wireless Mesh Routers Insufficient Entropy Vulnerability that was published October 23, 2012, on the ICS-CERT secure Portal library.

This advisory provides mitigation details for a vulnerability that impacts Tropos Wireless Mesh Routers. 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 SSH key generation in Tropos Networks's wireless network router product line. By impersonating the device, an attacker can obtain the credentials of administrative users and perform a Man-in-the-Middle (MitM) attack. Tropos has validated the vulnerability and produced an embedded operating software update that mitigates the reported vulnerability. According to Tropos, products are deployed across several sectors including the transportation, energy, water, emergency services, and critical manufacturing concentrated in the United States.

This vulnerability can be exploited remotely.

AFFECTED PRODUCTS

The following Tropos products are affected:

- All wireless mesh routers running Mesh OS versions prior to release 7.9.1.1

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 December 10, 2012.

This product is provided subject only to the Notification Section as indicated here: <http://www.us-cert.gov/privacy/>



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

IMPACT

An attacker can gain unauthorized access to the router by determining the authentication keys from reused or non-unique SSH host keys. By exploiting this vulnerability, the attacker can perform a MitM attack to affect the integrity of the data on the system.

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.

BACKGROUND

Tropos Networks is a US-based company. Tropos wireless mesh routers are used to build large scale, communication networks for aggregating multiple smart grids, industrial controllers, and fixed and mobile communication applications. According to Tropos, products are deployed across several sectors including the transportation, energy, water, emergency services, and critical manufacturing sectors. Tropos estimates that these products are used primarily in the United States (79% product deployment) and over 50 additional countries (21% total).

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSUFFICIENT ENTROPY^d

The Tropos products do not use sufficient entropy when generating keys for SSH connections, thereby making them weak. By calculating private authentication keys, an attacker could perform a MitM attack on the system by knowing the non-unique host key. This could enable the attacker to gain unauthorized access to the system and read information on the device, as well as inject data into the SSH stream compromising the integrity of the data.

CVE-2012-4898^e has been assigned to this vulnerability. A CVSS v2 base score of 6.1 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:P/A:N).^f

d. CWE 331, <http://cwe.mitre.org/data/definitions/331.html>, CWE-331: Insufficient Entropy, Web site last accessed December 10, 2012.

e. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4898>, 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=\(AV:N/AC:H/Au:N/C:C/I:P/A:N\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:H/Au:N/C:C/I:P/A:N)), Web site last accessed December 10, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a high skill would be able to exploit this vulnerability.

MITIGATION

Tropos Networks has released customer notification and an update (Tropos Mesh OS 7.9.1.1) for its network device embedded software. This update can be downloaded from the Tropos software download page.^g Download of the update requires a valid user name and password. The updated firmware fixes the vulnerability by using sufficient entropy to generate unique SSH host keys.

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.

g. Tropos Download Page, <http://support.tropos.com>, Web site last accessed December 10, 2012.

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed December 10, 2011.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click Web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email Scams^j for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks^k for more information on social engineering attacks.

ICS-CERT CONTACT

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

Email: ics-cert@hq.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.

i. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed December 10, 2012.

j. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed December 10, 2012.

k. National Cyber Alert System Cyber Security Tip ST04-014, <http://www.us-cert.gov/cas/tips/ST04-014.html>, Web site last accessed December 10, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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.