ICS-CERT ADVISORY

ICSA-12-243-01— GARRETTCOM— PRIVILEGE ESCALATION VIA USE OF HARD-CODED PASSWORD

August 30, 2012

OVERVIEW

Independent security researcher Justin W. Clarke of Cylance Inc. has identified a privilege-escalation vulnerability in the GarrettCom Magnum MNS-6K Management Software application via the use of a hard-coded password. This vulnerability could allow a remote attacker with any level of access to the system to escalate the attacker's privilege to the administrative level. The attacker must have access to a logon account on the device to exploit this vulnerability.

GarrettCom has produced a patch that mitigates this vulnerability.

AFFECTED PRODUCTS

The following GarrettCom products are affected:

- MNS-6K Rel, v4.1.14, and prior, and
- MNS-6K Rel, v14.1.14 SECURE and prior

IMPACT

Successful exploitation of this vulnerability from an established account on the system could allow escalation of privileges to full administrative access. The privilege escalation could provide the attacker a vector for making changes to settings, or initiating a complete device shutdown causing a denial of service (DoS).

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

GarrettCom is a US-based company that maintains offices in the US and Europe. The Magnum MNS-6K Management Software provides device management for the Magnum 6K line of managed Ethernet switches.

Resellers also offer GarrettCom products in South America, China, India, and the Middle East, however, GarrettCom estimates that the affected products are deployed primarily in the United States with a small percentage in Europe and Asia. According to GarrettCom, the 6K line of

switches are deployed across several U.S. critical infrastructure sectors including critical manufacturing, defense industrial base, energy, water, and transportation.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

USE OF HARD-CODED PASSWORD[a]

The Magnum MNS-6K Management Software uses an undocumented hard-coded password that could allow an attacker with access to an established device account to escalate privileges to the administrative or full-access level. While an attacker must use an established account on the device under attack, this vulnerability facilitates the circumvention of physical-connect safeguards and could allow complete administrative level access to the system, compromising system confidentiality, integrity, and availability.

CVE-2012-3014[b] has been assigned to this vulnerability. A CVSS v2 base score of 7.7 has been assigned; the CVSS vector string is (AV:A/AC:L/Au:S/C:C/I:C/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker with access to an established user account could remotely log into the affected system and elevate privileges to the administrative level, thereby circumventing the physical-connect safeguards in place for administrative functions.

EXISTENCE OF EXPLOIT

No known public exploit targets this vulnerability.

DIFFICULTY

An attacker with a low skill could exploit this vulnerability.

[a]. CWE, http://cwe.mitre.org/data/definitions/259.html , CWE-259: Use of Hard-Coded, Web site last accessed August 30, 2012.
[b]. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3014 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
[c]. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:A/AC:L/Au:S/C:C/I:C/A:C), Web site last accessed August 30, 2012.

MITIGATION

Despite this vulnerability not being documented in the May 18, 2012, release notes, GarrettCom has an updated software version that addresses this specific security vulnerability. Release notes and download information can be found at the following URLs:

http://www.garrettcom.com/techsupport/6k_dl/6k440_rn.pdf

http://www.garrettcom.com/techsupport/sw_downloads_6k.htm

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

- Remove or change any factory or default accounts on the device.
- Use strong password schemes for logon accounts.
- 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.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[d] 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-12-146-01A—Cyber Intrusion Mitigation Strategies,[e] 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.

ICS-CERT CONTACT

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

[d]. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed August 30, 2012.

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

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP 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.