ICS-CERT ADVISORY

ICSA-12-167-01—INNOMINATE MGUARD WEAK HTTPS AND SSH KEYS

June 15, 2012

OVERVIEW

An independent research group comprised of Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman identified an insufficient entropy vulnerability in Innominate's mGuard network appliance product line. By impersonating the device, an attacker can obtain the credentials of administrative users and potentially perform a Man-in-the-Middle (MitM) attack. Innominate has validated the vulnerability and produced an update that resolves the reported vulnerability. This vulnerability can be remotely exploited.

ICS-CERT has coordinated this vulnerability with Innominate, which has produced an update that resolves this vulnerability.[a]

AFFECTED PRODUCTS

All versions of the following Innominate products are affected:

- mGuard Smart—HW-101020, HW-101050, BD-101010, BD-101020,
- mGuard PCI—HW-102020, HW-102050, BD-111010, BD-111020,
- mGuard Industrial RS—HW-105000, BD-501000, BD-501010, BD-501020,
- mGuard Blade—HW-104020, HW-104050,
- mGuard Delta—HW-103050, BD-201000,
- EAGLE mGuard—HW-201000, BD-301010,
- All products manufactured prior to 2006.

a. Innominate Security Advisory 2012-06-14-001, http://www.innominate.com/data/downloads/software/innominate_security_advisory_20120614_001.pdf, Web site last accessed June 15, 2012.

IMPACT

This vulnerability can weaken the security posture of any industrial network in which these products are deployed.

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

Innominate is a company based in Berlin, Germany, founded in 2001. Innominate's mGuard product line includes firewall and VPN network security appliances. Innominate's products are deployed in many sectors including manufacturing, electric power generation, water, transportation, healthcare, communications, and satellite operations. Innominate reports that the mGuard products are used many countries worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSUFFICIENT ENTROPY[b]

The mGuard products do not use sufficient entropy when generating keys for HTTPS and SSH, therefore making them too weak. By calculating private keys, an attacker could perform a MitM attack on the system. This could allow the attacker to execute arbitrary code or gain unauthorized access to the system. Keys that are loaded as part of the mGuard configuration (i.e., VPN) are not affected.

CVE-2012-3006[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.1 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:S/C:C/I:C/A:C).[d]

b. CWE, http://cwe.mitre.org/data/definitions/331.html, CWE-331: Insufficient Entropy, Web site last accessed June 15, 2012.

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3006. NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:H/Au:S/C:C/I:C/A:C), Web site last visited June 15, 2012.

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker can predict the user's session ID and potentially hijack the session. This vulnerability could be exploited remotely by a MitM type attack. An attacker that has obtained unauthorized access could inject malicious code or change system settings.

The attacker must first successfully guess or calculate the private key of the mGuard device and have physical access to the network path between the device and a legitimate administrator or have the ability to deviate legitimate device traffic to the attacker's system using techniques such as ARP spoofing.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

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

MITIGATION

Software Version 7.5.0 or later properly uses existing entropy before generating HTTPS and SSH keys. It also increases the size of the RSA keys from 1,024 bits to 2,048 bits. The software update can be found at Innominate download website.[e] Innominate recommends changing passwords after new keys are generated.

Innominate recommends one of the three following mitigation procedures:

1. Use the Rescue Procedure to install the software Version 7.5.0. New keys will be generated as part of this process.
2. Use the update mechanism to update the devices to Version 7.5.0.
    a. Install the update. Existing keys will be kept.
    b. After the update, the existing keys must be replaced by using one of the following methods:
        i. Web User Interface
            1) Login as root or admin user.

e. Innominate Software Update Web site, http://www.innominate.com/en/services/software-updates, Web site last accessed June 15, 2012.

2) Press the "Generate new 2048 bit keys" button either in the "Web Settings -> Access" or in the "System Settings -> Shell Access" menu.
3) Note the fingerprint output of the newly generated keys.
4) Login via HTTPS and compare the certificate information provided by the browser.

ii. Console

1) Login via the serial console or SSH as root or admin user.
2) Call the program: *$ rsa_renewal update.*
3) Note the fingerprint output of the newly generated keys.
4) Login via SSH and compare the fingerprints shown by the SSH.

3. Upload and execute a shell script via SSH as root, provided by Innominate. The script will generate new 2,048 bit keys without requiring an update to software Version 7.5.0.
   a. The script can be downloaded from Innominate at http://www.innominate.com/en/downloads/software-and-misc.
   b. Use scp to copy the script onto the mGuard like (but appropriate for the user's setup): *$ scp generate_2048key.sh root@192.168.1.1:/root/.*
   c. Login via SSH as root user.
   d. Execute the script: *$ sh /root/generate_2048key.sh.*
   e. Note the fingerprint output of the newly generated keys.
   f. Login via SSH and compare the fingerprints shown by SSH.

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.

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

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 15, 2012.

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:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

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.