ICS-CERT ADVISORY

ICSA-12-212-02—SIEMENS SIMATIC S7-400 PN CPU DENIAL OF SERVICE VULNERABILITIES

July 30, 2012

OVERVIEW

Siemens has reported to ICS-CERT that denial-of-service (DoS) vulnerabilities exist in the SIMATIC S7-400 V6 and SIMATIC S7-400 V5 PN CPU products. Siemens has produced a firmware update that mitigates the vulnerability affecting the S7-400 V6.

Siemens will not fix the vulnerability that affects the S7-400 V5 because that product version has reached end-of-life and has been discontinued.

Both vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

Siemens reports that one of the vulnerabilities affects the following products within the S7-400 CPU family with firmware Versions 6.0.1 and 6.0.2

- CPU 412-2 PN (6ES7412-2EK06-0AB0)
- CPU 414-3 PN/DP (6ES7414-3EM06-0AB0)
- CPU 414F-3 PN/DP (6ES7414-3FM06-0AB0)
- CPU 416-3 PN/DP (6ES7416-3ES06-0AB0)
- CPU 416F-3 PN (6ES7416-3FS06-0AB0)

Another vulnerability affects the following products within the S7-400 CPU family with firmware Version 5:

- CPU 414-3 PN/DP (6ES7414-3EM05-0AB0)
- CPU 416-3 PN/DP (6ES7416-3ER05-0AB0)
- CPU 416F-3 PN/DP (6ES7416-3FR05-0AB0)

IMPACT

When specially crafted packets are received on Ethernet interfaces by the SIMATIC S7-400, the device can default into defect mode. A PLC in defect mode needs to be manually reset to return to normal operation.

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

Products in the Siemens SIMATIC S7-400 CPU family have been designed for process control in industrial environments such as manufacturing, power generation and distribution, food and beverages, and chemical industries worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DENIAL OF SERVICE[a]

When the Ethernet port on a SIMATIC S7-400 V6 receives a malformed IP packet, the device could go into the defect mode. The SIMATIC S7-400 V6 CPU defect mode locks out the unit so that it is not available for process control. An attacker could use this vulnerability to perform a DoS attack.

CVE-2012-3016[b] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[c]

DENIAL OF SERVICE[a]

When the Ethernet port on a SIMATIC S7-400 V5 receives a malformed IP or HTTP packet, the device could go into the defect mode. The SIMATIC S7-400 V5 CPU defect mode locks out the unit so that it is not available for process controls. Attackers may use this vulnerability to perform a denial-of-service attack.

CVE-2012-3017[d] has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).[e]

a. CWE-404: Improper Resource Shutdown or Release, http://cwe.mitre.org/data/definitions/404.html, Web site last accessed July 30, 2012.
b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3016, 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:N/AC:L/Au:N/C:N/I:N/A:C), Web site last visited July 30, 2012.
d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-30167, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker with a low skill could exploit these vulnerabilities.

MITIGATION

Siemens has released security advisories (SSA-589272 and SSA-617264)[f] that detail the vulnerabilities in the tw SIMATIC S7-400 CPU and the recommended security practices to secure the systems.

Siemens provided firmware update V6.0.3[g,h,i] that closes the vulnerability affecting the S7-400 V6 by fixing the flawed packet processing implementation.

Siemens is not providing a firmware update for SIMATIC S7-400 V5 PN CPUs because this version has reached end-of-life and has been discontinued.

ICS-CERT encourages asset owners to take the following 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.

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

f Siemens Security Advisories, http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm, Website last visited July 30, 2012.

g. CPU 412-2 PN, http://support.automation.siemens.com/WW/view/en/45645157, Website last visited July 26, 2012.

h. CPU 414-3 PN/DP, CPU 414F-3 PN/DP, http://support.automation.siemens.com/WW/view/en/45645228, Website last visited July 30, 2012.

i. CPU 416-3 PN/DP, CPU 416F-3 PN, http://support.automation.siemens.com/WW/view/en/45645229, Website last visited July 30, 2012.

- 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.[j] 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,[k] which 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:

Email: 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

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

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

development of proper mitigations may put industrial control systems and the public at avoidable risk.