



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-305-01—SIEMENS SIPASS SERVER BUFFER OVERFLOW

October 31, 2012

OVERVIEW

This advisory provides mitigation details provided by Siemens for a vulnerability that impacts the Siemens SiPass server.

Siemens has reported^a a buffer overflow vulnerability in Siemens' SiPass server. Lucas Apa of IOActive discovered this vulnerability and reported it directly to Siemens. Siemens has provided mitigations and a software hotfix corrects this vulnerability. Exploitation of this vulnerability would allow an attacker to perform a denial of service (DoS) and possibly gain access to the system via remote code execution.

This vulnerability can be exploited remotely.

AFFECTED PRODUCTS

Siemens reports that the vulnerability affects the following versions of SiPass:

- SiPass integrated MP2.6 and earlier.

IMPACT

Attackers exploiting this vulnerability may perform a DoS attack or possibly access the system via remote code execution.

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

BACKGROUND

Siemens AG is a multinational company headquartered in Munich, Germany. Siemens' principal activities are in the fields of industry, energy, transportation, and healthcare.

a. SSA-938777: Possible Remote Code Execution in SiPass integrated, <http://www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm>, Web site last accessed October 31, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

SiPass integrated is a Windows-based client/server system with a wide range of access control and security features. One component of SiPass integrated is SiPass server that is used for central system management.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW^b

By sending a specially crafted packet to Port 4343/TCP, an attacker can cause a DoS condition with possible remote code execution. The SiPass server accepts these messages and incorrectly processes them, causing the affected conditions. No authentication is required to access this affected network port.

CVE-2012-5409^c has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).^d

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

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

MITIGATION

Siemens has provided a software hotfix^a resolving the vulnerability for customers of SiPass integrated MP2.4, MP2.5, and MP2.6. Please contact Siemens customer support^e for acquiring

b. CWE-121: Stack-based Buffer Overflow, <http://cwe.mitre.org/data/definitions/121.html>, Web site last accessed October 31, 2012.

c. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5409>, 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=\(AV:N/AC:L/Au:N/C:C/I:C/A:C\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C)), Web site last visited October 31, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

this hotfix. Siemens recommends customers with earlier versions of SiPass integrated to upgrade to one of the above mentioned versions. In addition, perimeter firewalls may be configured to block Port 4343/TCP to SiPass server.

The affected software components are implemented under the assumption of running in a protected IT environment. Siemens strongly recommends protecting systems according to common security practices.

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.^f 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,^g 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.

e. Siemens Customer Support, misp.support.de@siemens.com.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 31, 2012.

g. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed October 31, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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.