ICS-CERT ADVISORY

ICSA-12-227-01—SIEMENS COMOS DATABASE PRIVILEGE ESCALATION VULNERABILITY

August 14, 2012

OVERVIEW

Siemens has reported a privilege escalation vulnerability in the Siemens COMOS database application. Siemens has produced an update that fixes this vulnerability. This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

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

- all versions earlier than Version 9.1,
- Version 9.1: Patch 412 and earlier,
- Version 9.2: Update 3 Patch 022 and earlier, and
- Version 10: Patch 004 and earlier.

IMPACT

Authenticated users with read privileges could escalate their privileges by exploiting this vulnerability. Thus, the attacker is able to gain administrator access to the database.

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

Siemens COMOS[a] is an object oriented database system that supports collecting, processing, saving, and distributing of information through a design process. It allows the configuration of different user privileges to different users.

a. Siemens COMOS Software, http://www.siemens.com/comos, Web site last accessed August 14, 2012.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

PRIVILEGE ESCALATION[b]

Authenticated users with read privileges could escalate their privileges by exploiting a documented method in the design of the database. As a result, the attacker gains administrator access to the database.

CVE-2012-3009[c] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:S/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 medium skill level could exploit these vulnerabilities.

MITIGATION

For COMOS Versions 9.1, 9.2, and 10.0, Siemens[e] recommends installing the corresponding patches as soon as possible:

- Version 9.1 Patch 413,
- Version 9.2 Update 03 Patch 023, and

b. CWE-250: Execution with Unnecessary Privileges, http://cwe.mitre.org/data/definitions/122.html, Web site last accessed August 14, 2012.

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3009, 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:M/Au:S/C:C/I:C/A:C) , Web site last accessed August 14, 2012.

e. Siemens Security Advisories, http:/www.siemens.com/corporate-technology/en/research-areas/siemens-cert-security-advisories.htm, Web site last accessed August 14, 2012.

- Version V10 Patch 005.

These software updates are available at Siemens customer support.[f] For earlier versions, Siemens recommends upgrading to a newer version.

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.[g] 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,[h] 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:

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

f. Siemens Industry Online Support, http://support.automation.siemens.com/WW/view/en/31495514, Web site last accessed August 14, 2012.

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed August 14, 2012.

h. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed August 14, 2012.

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.