ICS-CERT ADVISORY

ICSA-12-201-01—OSISOFT PI OPC DA INTERFACE BUFFER OVERFLOW

July 19, 2012

OVERVIEW

ICS-CERT has received a report from OSIsoft concerning a stack-based buffer overflow in the PI OPC DA Interface software that could cause the software to crash or allow a remote attacker to execute arbitrary code. This vulnerability was discovered during a software assessment requested by OSIsoft and funded by the US Department of Homeland Security.

OSIsoft has published a customer notification, and has released a product update that resolves this vulnerability.

AFFECTED PRODUCTS

The vulnerability affects all versions of PI OPC DA Interface prior to Version 2.3.20.9.

IMPACT

Successful exploitation of this vulnerability could allow a remote, authenticated attacker to execute arbitrary code on a vulnerable system.

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

According to OSIsoft, PI OPC DA Interface allows the PI System to access plant floor process data using the OPC standard.

VULNERABILITY OVERVIEW

STACK-BASED BUFFER OVERFLOW[a]

The PI OPC DA Interface does not correctly validate the OPC input messages before performing further processing. By sending additional valid packets, an attacker could partially control corruption to force the arbitrary freeing of a memory address. This could allow the attacker to cause a crash or to execute arbitrary code.

CVE-2012-3008[b] has been assigned to this vulnerability. A CVSS v2 base score of 6.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:S/C:N/I:N/A:C). [c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be exploited remotely by an authenticated attacker with the ability to write data to OPC items collected by the PI OPC DA Interface.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would require a medium skill level.

MITIGATION

OSIsoft has produced an update that resolves this vulnerability. OSIsoft encourages customers using the affected products to upgrade to Version 2.3.20.9 or later. The PI OPC DA Interface update can be found at the OSIsoft technical support Web site.[d]

a. CWE, http://cwe.mitre.org/data/definitions/121.html, CWE-121: Stack-based Buffer Overflow, Web site last accessed July 18, 2012.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3008 , 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:M/Au:S/C:N/I:N/A:C), Web site last visited July 19, 2012.

d. OSIsoft, http://techsupport.osisoft.com, Web site last accessed July 19, 2012.

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.[e] In addition, ICS-CERT has published a standalone document for general mitigation strategies (ICS-TIP-12-146-01),[f] which can be downloaded from the ICS-CERT Web page. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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/.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed July 19, 2012.

f. ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web page last accessed July 19, 2012.

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.