ICS-CERT ADVISORY

ICSA-12-258-01—IOSERVER OPC SERVER MULTIPLE VULNERABILITIES

September 14, 2012

OVERVIEW

Independent researcher Hinge of foofus.net has identified multiple vulnerabilities[a] in IOServer's OPC Server application. IOServer has released a new version of the product that partially mitigates these vulnerabilities. Hinge has tested the new version and found that it partially resolves these vulnerabilities. These vulnerabilities can be exploited remotely. Exploits that target these vulnerabilities are known to be publicly available.

AFFECTED PRODUCTS

The following IOServer OPC Server versions are affected:

- IOServer OPC Server 1.0.18.0 and earlier.

IMPACT

These vulnerabilities allow an attacker to download any file on the file system without authentication.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

IOServer is an Australia-based company that produces the affected product, OPC Server, which is designed to exchange data between the human-machine interface and the programmable logic controllers. According to IOServer, OPC Server is deployed across several sectors including

a. IOServer "Root Directory" Trailing Backslash Web Server Vuln, http://www.foofus.net/?page_id=616, Web site last accessed September 13, 2012.

manufacturing, building automation, oil and gas, and electric utilities. IOServer estimates that these products are used primarily in the United States and Europe with a small percentage in Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CVE-2012-4680[b] has been assigned to these three closely related vulnerabilities. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:N/A:N).[c]

1. INSUFFICIENT ACCESS CONTROLS[d]

The application stores sensitive data under the Web document root with insufficient access control, which might make it accessible to unauthorized parties.

2. DIRECTORY LISTING[e]

The product stores sensitive information in files or directories that are accessible to actors outside of the intended control sphere.

3. DIRECTORY TRAVERSAL[f]

The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. However, the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. This allows arbitrary access to any file on the server.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4680, 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:C/I:N/A:N), Web site last accessed September 13, 2012.

d. CWE-219: Sensitive Data Under Web Root, http://cwe.mitre.org/data/definitions/219.html, Web site last accessed September 13, 2012.

e. CWE-538: File and Directory Information Exposure, http://cwe.mitre.org/data/definitions/538.html, Web site last accessed September 13, 2012.

f. CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), http://cwe.mitre.org/data/definitions/22.html, Web site last accessed September 13, 2012.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

Exploits that target these vulnerabilities are publicly available.

DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities.

MITIGATION

IOServer has created a new version (Version 1.0.19.0[g]) to correct the directory traversal vulnerability (Vulnerability #3 above). The researcher has found that this new version still contains insufficient access controls (Vulnerability #1) and allows directory listings (Vulnerability #2) inside the root directory and its subdirectories.

In addition to the patch, the researcher recommends that users ensure that the "Root Directory" configuration value has a trailing backslash. This helps to mitigate the remaining issues, although an attacker can still get a directory listing of the root directory itself (but not subdirectories) with this in place.

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

g. IOServer version 1.0.19.0, http://www.ioserver.com/driver19.exe, Web site last accessed September 13, 2012.

Cybersecurity with Defense-in-Depth Strategies.[h] 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-12-146-01—Cyber Intrusion Mitigation Strategies,[i] 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:

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

h. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 13, 2012.

i. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 13, 2012.