ICS-CERT ADVISORY

ICSA-12-271-02—OPTIMALOG OPTIMA PLC MULTIPLE VULNERABILITIES

September 27, 2012

OVERVIEW

Independent researcher Luigi Auriemma identified a NULL Pointer Dereference and an Infinite Loop and released proof-of-concept (exploit) code for Optimalog's Optima PLC application without coordination with ICS-CERT, the vendor, or any other coordinating entity known to ICS-CERT.

Optimalog has released a new version to address these vulnerabilities. The component APIFTP is no longer installed by default with Optima PLC, the user must check a specific option. A security warning is displayed at the first performance of APIFTP to inform the user about opening a TCP port and asking the user to validate APIFTP use.

AFFECTED PRODUCTS

The following Optimalog Optima PLC Versions are affected:

- Optima PLC 1.5.2 and prior.

IMPACT

Successful exploitation of these vulnerabilities may result in a denial of service (DoS).

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

Optimalog is a France-based company. The affected product, Optima PLC, is a software-based PLC system. This product is used primarily in Europe.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

NULL POINTER DEREFERENCE[a]

By sending a specially crafted packet to a specific port, Optima PLC’s component APIFTP will dereference a NULL Pointer when using path names that are long. This will result in termination of the server.

CVE-2012-5048[b] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:P).[c]

LOOP WITH UNREACHABLE EXIT CONDITION[d]

By sending a specially crafted packet to a specific port, Optima PLC’s component APIFTP does not correctly handle incomplete packets. This will result in an infinite loop being called that will cause CPU consumption and may result in a DoS.

CVE-2012-5049[e] has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:P).[f]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

[a] CWE, http://cwe.mitre.org/data/definitions/476.html, CWE-476: NULL Pointer Dereference, Web site last accessed September 26, 2012.

[b] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5048, 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:P), Web site last accessed September 26, 2012.

[d] CWE, http://cwe.mitre.org/data/definitions/835.html, CWE-835: Loop with Unreachable Exit Condition, Web site last accessed September 26, 2012.

[e] NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5049, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

[f] CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:P), Web site last accessed September 26, 2012.

EXISTENCE OF EXPLOIT

Exploits that target this vulnerability are publicly available.

DIFFICULTY

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

MITIGATION

Optimalog's recommendation to all users that plan to use APIFTP Server is to configure their firewall and VPN accordingly and set the program to run at startup of the station. If a user does not plan to use APIFTP server, then disable its execution.

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 a 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.[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.

[g] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed September 26, 2012.

[h] Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed September 26, 2012.

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 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.