ICS-CERT ADVISORY

ICSA-12-179-01—PRO-FACE PRO-SERVER EX MULTIPLE VULNERABILITIES

June 27, 2012

OVERVIEW

This advisory is a follow-up to the alert titled "ICS-ALERT-12-137-01 - Pro-face Pro-Server EX Multiple Vulnerabilities," that was published May 16, 2012, on the ICS-CERT Web page.

Independent researcher Luigi Auriemma identified multiple vulnerabilities in the Pro-face Pro-Server application and publicly released this information without coordination with ICS-CERT, the vendor, or any other coordinating entity known to ICS-CERT.

The four confirmed vulnerabilities are invalid memory access, integer overflow, unhandled exception, and memory corruptions. Each of these vulnerabilities are remotely exploitable, and public exploits are known to target these vulnerabilities.

ICS-CERT has coordinated these vulnerabilities with the development and manufacturing company of Pro-face branded products, Digital Electronics, which has produced an update that resolves these vulnerabilities.

AFFECTED PRODUCTS

Digital Electronics reports that the vulnerabilities affect the following products.

- data management software Pro-Server EX versions 1.00.00 through 1.30.00, and
- HMI screen editor and logic programming software GP-Pro EX and related software WinGP Versions 2.00.00 through 3.01.100.

IMPACT

Exploitation of the reported vulnerabilities can result in a denial of service (DoS) or arbitrary code execution.

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

Pro-face is HMI-related hardware and software product found in a wide range of industries such as oil and gas, food and beverage, and water and wastewater industries. Pro-face products are used throughout the world, the highest number sold in Japan and the Asian Pacific area. According to its Web site, Pro-Server EX is a data management server that collects information generated by a PLC system through an HMI unit and generates reports. In February 2001, Pro-face America, Inc., a subsidiary of Digital Electronics Corporation, purchased Xycom Automation.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

MEMORY CORRUPTION[a]

A specially crafted packet can cause an integer overflow that leads to a buffer overflow in an arbitrary memory location. Out-of-bounds memory access may result in the corruption of memory or instructions that may lead to a crash. The execution of arbitrary code may be possible. Other attacks leading to lack of availability may also be possible.

CVE-2012-3792[b] has been assigned to this vulnerability. A CVSS v2 base score of 5.8 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:N/A:P).[c]

INTEGER OVERFLOW[d]

It is possible to exploit an integer overflow to crash the server which could be considered a denial of service.

CVE-2012-3793[e] has been assigned to this vulnerability. A CVSS v2 base score of 4.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N/A:P).[f]

a. CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, http://cwe.mitre.org/data/definitions/119.html, Web site last accessed June 27, 2012.
b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3792, Web site last visited June 27, 2012.
c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:P/I:N/A:P), Web site last visited June 27, 2012.
d. CWE-680: Integer Overflow to Buffer Overflow, http://cwe.mitre.org/data/definitions/680.html, Web site last accessed June 27, 2012.
e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3793, Web site last visited June 27, 2012.
f. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last visited June 27, 2012.

UNHANDLED EXCEPTION[g]

It is possible to terminate the server because of an unhandled exception. Exploitation of this vulnerability will cause a denial-of-service condition.

CVE-2012-3794[h] has been assigned to this vulnerability. A CVSS v2 base score of 4.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:N/A:P).[i]

INVALID MEMORY READ ACCESS[j]

An attacker may crash the server by copying a large amount of memory from the target system.

CVE-2012-3795[k] and CVE-2012-3796[l] have been assigned to these vulnerabilities. A CVSS v2 base score of 5.8 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:N/A:P).[m]

MEMORY CORRUPTIONS[n]

An attacker is able to write more data to a memory location than is allocated due to a lack of size checks. This will likely result in a system crash.

CVE-2012-3797[o] has been assigned to this vulnerability. A CVSS v2 base score of 4.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:N/I:P/A:N).[p]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities can be remotely exploited.

g. CWE-388: Error Handling, http://cwe.mitre.org/data/definitions/388.html, Web site last accessed June 27, 2012.
h. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3794, Web site last accessed June 27, 2012.
i. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last visited June 27, 2012.
j. CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer, http://cwe.mitre.org/data/definitions/119.html, Web site last accessed June 27, 2012.
k NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3795, Web site last accessed June 27, 2012.
l. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3796, Web site last accessed June 27, 2012.
m. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last visited June 27, 2012.
n. CWE-788: Access of Memory Location After End of Buffer, http://cwe.mitre.org/data/definitions/788.html, Web site last accessed June 27, 2012.
o. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3797, Web site last accessed June 27, 2012.
p. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:C/I:C/A:C), Web site last visited June 27, 2012.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

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

MITIGATION

Digital Electronics has released patch modules on its Web site at the following location: http://www.pro-face.com/news/2012/0606.html.

The patch module prevents the Pro-Server EX and WinGP from an attack using inaccurate packets.

Digital Electronics recommends the following in addition to applying the patch:

- Review all network configurations for control system devices.
- Remove unnecessary PCs from control system networks.
- Remove unnecessary applications from control system networks.

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.[q] 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.

q. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 27, 2012.

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

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.