ICS ADVISORY

Orpak SiteOmat

Last Revised: May 06, 2019 **Alert Code:** ICSA-19-122-01

1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit/public exploits available
- **Vendor:** Orpak (acquired by Gilbarco Veeder-Root)
- **Equipment:** SiteOmat
- **Vulnerabilities:** Use of Hard-coded Credentials, Cross-site Scripting, SQL Injection, Missing Encryption of Sensitive Data, Code Injection, Stack-based Buffer Overflow

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could result in arbitrary remote code execution resulting in possible denial-of-service conditions and unauthorized access to view and edit monitoring, configuration, and payment information.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of SiteOmat, software for fuel station management, are affected:

- SiteOmat versions prior to 6.4.414.122 only are vulnerable to stack-based buffer overflow CVE-2017-14854 and Code Injection CVE-2017-14853
- SiteOmat Versions prior to 6.4.414.084

3.2 VULNERABILITY OVERVIEW

3.2.1 USE OF HARD-CODED CREDENTIALS CWE-798

<https://cwe.mitre.org/data/definitions/798>

The application utilizes hard coded username and password credentials for application login.

CVE-2017-14728 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:h/a:h>).

3.2.2 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING') CWE-79

<https://cwe.mitre.org/data/definitions/79.html>

The application web interface does not properly neutralize user-controllable input, which could allow cross-site scripting.

CVE-2017-14850 has been assigned to this vulnerability. A CVSS v3 base score of 6.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:r/s:c/c:l/i:l/a:n>).

3.2.3 IMPROPER NEUTRALIZATION OF SPECIAL ELEMENTS USED IN AN SQL COMMAND ('SQL INJECTION') CWE-89

<https://cwe.mitre.org/data/definitions/89.html>

The application does not properly sanitize external input, which may allow an attacker to access the product by specially crafted input.

CVE-2017-14851 has been assigned to this vulnerability. A CVSS v3 base score of 9.4 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:h/a:l>).

3.2.4 MISSING ENCRYPTION OF SENSITIVE DATA CWE-311

<https://cwe.mitre.org/data/definitions/311.html>

The application transmits information in plain text, including credentials, which could allow an attacker with access to transmitted data to obtain credentials and bypass authentication.

CVE-2017-14852 <https://nvd.nist.gov/vuln/detail/cve-2017-14852> has been assigned to this vulnerability. A CVSS v3 base score of 8.6 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:l/a:l>).

3.2.5 IMPROPER CONTROL OF GENERATION OF CODE ('CODE INJECTION') CWE-94 <https://cwe.mitre.org/data/definitions/94.html>

The application does not properly restrict syntax from external input, which could allow unauthenticated users to execute specially crafted code on the target system.

CVE-2017-14853 <https://nvd.nist.gov/vuln/detail/cve-2017-14853> has been assigned to this vulnerability. A CVSS v3 base score of 8.6 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:l/i:h/a:l>).

3.2.6 STACK-BASED BUFFER OVERFLOW CWE-121

<https://cwe.mitre.org/data/definitions/121.html>

The application utilizes a function that accepts user input. This input is not properly validated, which could allow an attacker to execute arbitrary code.

CVE-2017-14854 has been assigned to this vulnerability. A CVSS v3 base score of 9.1 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H) <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:n/i:h/a:h>.

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Commercial Facilities, Energy, Transportation Systems
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Israel

3.4 RESEARCHER

Ido Naor and Amihai Naiderman of Kaspersky Lab reported these vulnerabilities to NCCIC.

4. MITIGATIONS

Orpak recommends users of affected versions update to the latest release v6.4.414.139 or later. The update can be obtained by contacting customer care with the following options:

Online Ticket (login required): https://support.zoho.com/portal/orpak/home <https://support.zoho.com/portal/orpak/home>

Email: support@orpak.com

Tel: +972 3 577 6864

NCCIC recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet </ics/alerts/ics-alert-10-301-01>.
- 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 VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.
- Restrict system access to authorized personnel only and follow a least privilege approach.
- Apply defense-in-depth strategies.
- Disable unnecessary accounts and services.

NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

NCCIC also provides a section for control systems security recommended practices </ics/content/recommended-practices> on the ICS-CERT web page. Several recommended

practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS-CERT website </ics/> in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to NCCIC for tracking and correlation against other incidents.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Orpak

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top