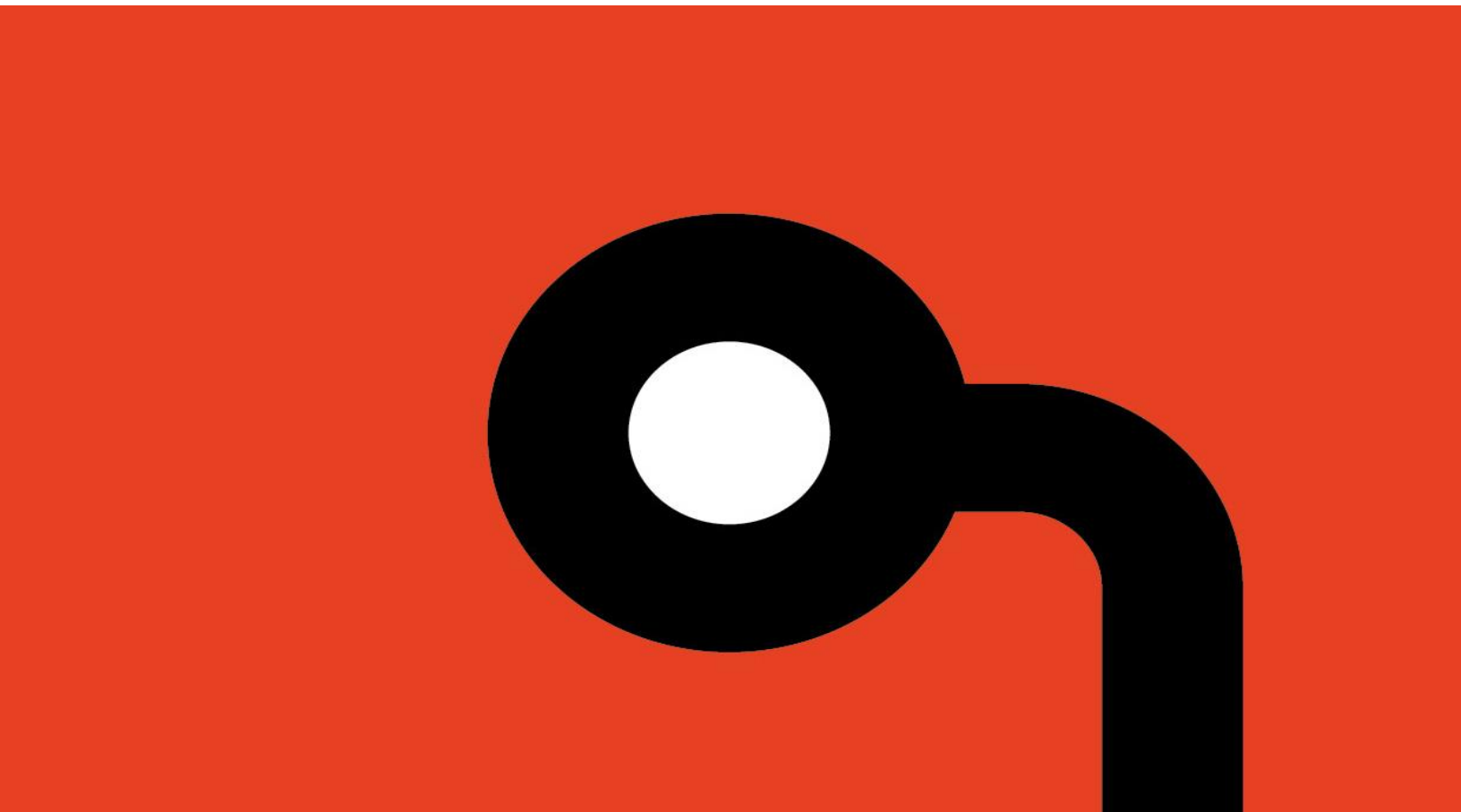
Applied Risk

AR2019008

Optergy Proton / Enterprise 2.3.0a Multiple Vulnerabilities

Author: Gjoko Krstic

Release Date: May 10, 2019



Copyright Notices

OVERVIEW

Multiple vulnerabilities were found in the Optergy Proton / Enterprise Building Management System (BMS). These findings include Open Redirect, Username Disclosure, Cross-Site Request Forgery, Unrestricted File Upload, Backdoor Console, Internal Network Information Disclosure, SMS Sending Service and Hard-coded Credentials.

AFFECTED PRODUCTS

Optergy Proton / Enterprise;

The following versions are affected:

- 2.3.0a and bellow

The vulnerabilities have been discovered and validated in Optergy Proton / Enterprise 2.3.0a. Older versions are affected too.

IMPACT

An unauthenticated user can have full system access.

BACKGROUND

Optergy is a technology company dedicated to the business of managing buildings, facilities and enterprises with tools to improve efficiency, performance and processes, whilst providing key stakeholders with the information and reporting to make strategic decisions. Optergy Building Management System (BMS), is software that allows users to monitor and control equipment within a building.

VULNERABILITY DETAILS

Open Redirect

Input passed to the ‘url’ variable when calling the updating() function in ‘updating.jsp’ script is not properly verified before being used to redirect users. This can be exploited to redirect a user to an arbitrary website e.g. when a user clicks a specially crafted link to the affected script hosted on a trusted domain.

Applied Risk has calculated a CVSSv3 score of 3.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N.

Cross-Site Request Forgery

The affected application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.

Applied Risk has calculated a CVSSv3 score of 5.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L.

Unrestricted File Upload

The vulnerability exists due to the absence of file extension validation when uploading files through the badge image upload script. A remote and unauthenticated attacker can upload files with arbitrary extension into a directory within application's web root and execute them with privileges of the web server.

Applied Risk has calculated a CVSSv3 score of 9.9 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H.

Information Disclosure

The application suffers from username disclosure via its username reset functionality. An attacker can enumerate and disclose all the valid users on the system. Furthermore, when calling the http://TARGET/GetIPAddress.html page from remote location, the following internal information can be divulged for the current system: Name, Internal IP Address, Netmask, Hostname, Gateway, DNS Server and DNS Server 2.

Applied Risk has calculated a CVSSv3 score of 5.3 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

Hard-coded Credentials and SMS Sending Service

The SMSCetralTest.class doesn't have the PrivilegeName[] getRequiredPrivileges() function declared. This allows unauthenticated users to access this resource directly. Attackers can use this to send unauthorized SMS messages to any phone number depending of the stored credits to the hard-coded credentials in the sendMessage() function.

Applied Risk has calculated a CVSSv3 score of 7.3 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L.

Backdoor Console

The application suffers from an unauthenticated code execution with highest privileges. Attackers can exploit this issue by directly navigating to an undocumented backdoor script called Console.jsp in the tools directory and gain full system access.

Applied Risk has calculated a CVSSv3 score of 10.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

MITIGATION

Optergy is aware of the reported vulnerabilities and has addressed the issues with new firmware version.

REFERENCES

Vendor website

https://www.optergy.com/

Product page

https://optergy.com/products/proton/
https://optergy.com/products/optergy-enterprise/

Common Vulnerability Exposure (CVE):

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7272
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7273
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7274
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7275
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7276
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7277
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7278
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7279

Vendor New Version Release:
https://controltrends.org/building-automation-and-integration/05/optergy-new-enterprise-v-2-4-5-has-been-released/

CONTACT DETAILS

For any questions related to this report, please contact Applied Risk Research team at:

Email: research@applied-risk.com

PGP Public Key:


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFOgiBQBCACj+Notofe/liuHuc90yy8GAfFn8YFCsMCo7wQmQRNTT43bZQq2
gQr7FTLtOl6rBkOLm8bDk0YY/CtWsjdLh1jlDrWyfU6yIzfcu4CSpn1+5n1ivNN5
17ri+VtmgF392twiKhy2+MC9O4of+GMyu1hy5pIjwi3qGzdNlAnT7m7U/hNzaIR4
ae7+NuWtEvWWKyp3IEEMKTDV/ZOtRD1tfIR8KeBB7Axa8cJdlotw/Ail9TLVB6kt
a/BlvhM/zgWfbEPadnx6B0u7pdW50bTECAs0VHje8mcheTwTCAJo+de3/DqUA34X
oF9aAZWpZWE7VH0O4Q8ZtfrXPFqR2xF8LHhZABEBAAG0REFwcGxpZWQgUmlzayBS
ZXNlYXJjaCBUZWFtIChubyBwYXNzd29yZCkgPHJlc2VhcmNoQGFwcGxpZWQtcmlz
ay5jb20+iQE+BBMBAgAoBQJToIgUAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgID
AQIeAQIXgAAKCRA6nyA79MpeSay8CACSI4UhAget5Z+qEDmz1fe+9krgmx7wwDnF
ig4AVICU8ppJQoUCB5pP6eIV/DM7i+mu8e9zeGlA82t69yTVIANWx72zPmGn5Ku8
4t79gR8V+99PW+O+1rej+96wfL2v+IuOXOcJkTsheUyQZ8Klwc1U8kTdGZEY+/IZ
c32ZhyJ04/cchVP/Zsj2WQIh84wbqa27bTEyyFBnD8FdQ2R4UDTqwACbLgp82m29
P346s80c15RZIX8wUAu0LcNbWJJHRsX6Sa+MozTNug9yWdpZt+nmHEMl95lJYktR
w3+gwyaXeUxALX8Baq2EJDdNx9OlsryiNFdnE9vKIM0+24fTDoqguQENBFOgiBQB
CACtSAm5oBD4kJJY+rtHh6xoytOzP6bFEnrVjqXrXCj+ECG6+N6Droqd072X5hki
qoL1viI4NV+2jrYTtMIu+/nc4zuUFUDRYSm0X/K3WgsqaLA4jdedTm45Tau/Fn6W
26tB5AaddcoDdx6JVGIxFvwU+41KoZ7ouDZo7UEBZ7getPubyR4aPepUsjYnPOUL
0SHH76+b/pC5AZm4crpqWf7Q+qaYQdBIhJbgm5ijFzCyHusYgVGBT1hak81QGpM0
1K9wXki/fJrRyEsWWUjpVSEPRizsFJ60v+NrX50gvvXed8MlX0O9efwgeCmGIVDL
oxF/AmnznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd
-----END PGP PUBLIC KEY BLOCK-----
```