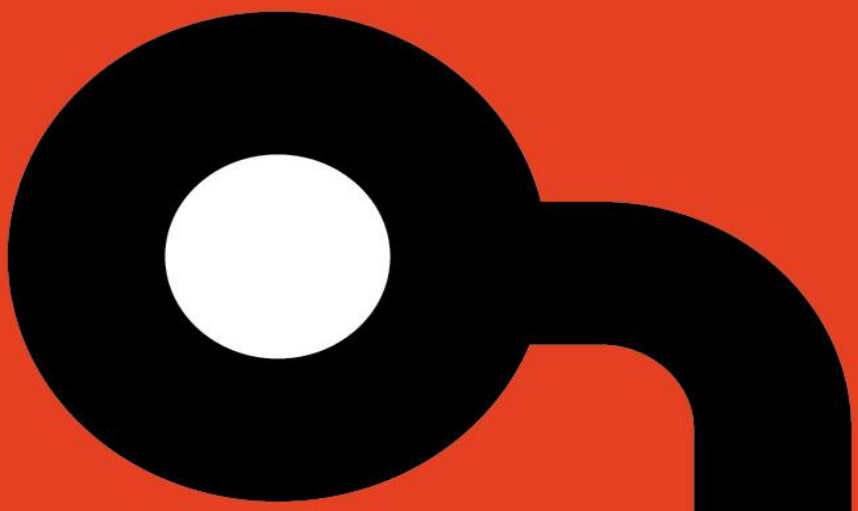
Applied Risk

AR2018001

Schneider Electric EcoStruxure™ Machine Experts' SoMachine Basic 1.6.0 XXE OOB Remote Arbitrary Data Retrieval

Author: Gjoko Krstic

Release Date: May 22, 2018



Confidentiality and Copyright Notices

Confidentiality

COPYRIGHT NOTICE AND CONFIDENTIALITY STATEMENT

OVERVIEW

An unauthenticated remote XML External Entity processing vulnerability has been discovered by researchers of Applied Risk. This affects the Schneider Electric SoMachine Basic 1.6.0 software, used in PLC configuring and developing automation machinery. Currently, there are no known public exploits targeting this vulnerability in said solution.

AFFECTED PRODUCTS

EcoStruxure Machine Expert product range; SoMachine Basic;

The following versions are affected:

- SoMachine Basic 1.6.0 build 61653
- SoMachine Basic 1.5.5 SP1 build 60148

The vulnerability has been discovered and validated on SoMachine 1.6.0 build 61653 and SoMachine Basic 1.5.5 SP1 build 60148. Older versions are probably affected too.

IMPACT

An unauthenticated user can craft a malicious project and/or template file that will enable her to read arbitrary files within the context of an affected system allowing disclosure of valuable information via out of band channels. An attack could include disclosure of sensitive local files including password data, private user data or relative paths in the system identifier.

BACKGROUND

Schneider Electric SE is a European multinational corporation that specializes in energy management, automation solutions, spanning hardware, software, and services. SoMachine is a professional, efficient and open Original Equipment Manufacturers (OEM) software solution that aides you in the developing, configuring and commissioning of the entire machine in a single environment including logic, motor control, HMI and related network automation functions.

VULNERABILITY DETAILS

XML External Entity (XXE) Processing

The application suffers from an XML External Entity (XXE) vulnerability using the DTD parameter entities technique resulting in disclosure and retrieval of arbitrary data on the affected node via out-of-band (OOB) attack.

The vulnerability is triggered when input passed to the XML parser is not sanitized while parsing the XML project and/or template file. This attack can also be used to execute arbitrary code (in certain circumstances, depending on the platform) or cause a denial of service (DoS) condition (billion laughs) via a specially crafted XML file including multiple external entity references.

Applied Risk has calculated a CVSSv3 score of 8.6 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H.

MITIGATION

Schneider Electric addressed the reported vulnerability by releasing a new version (v1.6 SP1) update for the affected software. Customers should update to the latest version to prevent any potential future exploitations. The updates are available at the following link:

https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP1/

REFERENCES

Vendor website

http://www.schneider-electric.com

Product page

https://www.schneider-electric.com/en/product-range/2226-ecostruxure%E2%84%A2-machine-expert?subNodeId=314728896en_WW

Schneider Electric Advisory (SEVD-2018-142-01)

https://www.schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp

Common Vulnerability Exposure (CVE) ID CVE-2018-7783

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7783
https://nvd.nist.gov/vuln/detail/CVE-2018-7783

OWASP

https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Processing

Common Weakness Enumeration (CWE) definition 611

https://cwe.mitre.org/data/definitions/611.html

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-----
```