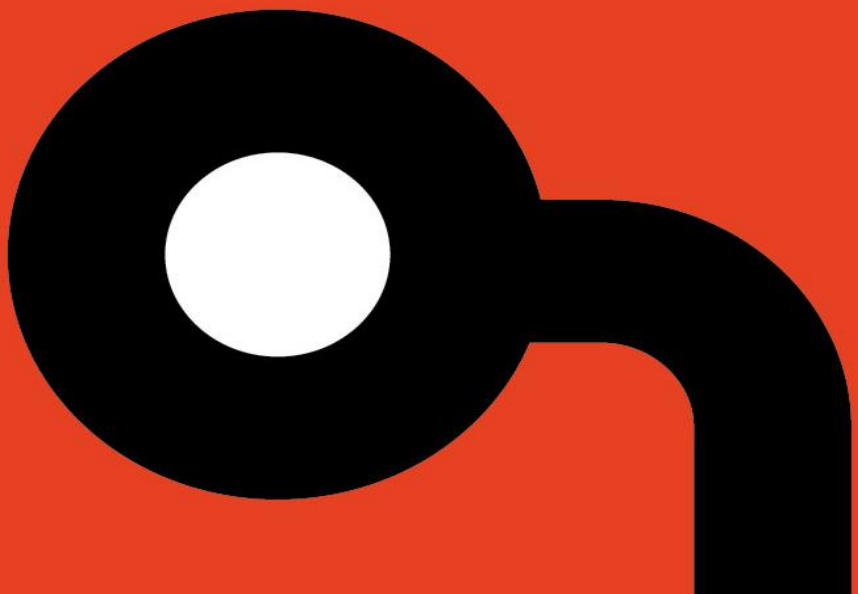
Applied Risk

AR2018005

SAUTER CASE Suite XML External Entity Injection Remote Arbitrary Data Retrieval

Author: Gjoko Krstic

Release Date: November 2, 2018



Copyright Notice

OVERVIEW

An unauthenticated remote XML External Entity processing vulnerability has been discovered in SAUTER CASE Suite 3.3 software used for handling building automation projects. There are no known public exploits targeting this vulnerability in said solution.

AFFECTED PRODUCTS

SAUTER CASE Components, SAUTER CASE Sensors, CAUTER CASE VAV

The following versions are affected:

- Program version: 3.10 and prior
- Program version: 3.3.1.1, Devices DB version: 6.13

The vulnerability has been discovered and validated on SAUTER CASE Suite 3.10. Older versions are probably affected too.

IMPACT

An unauthenticated user can craft a malicious XML data file that will enable them to read arbitrary files within the context of an affected system allowing disclosure of valuable information via out of band channels.

BACKGROUND

SAUTER puts you on course for energy efficiency and injects new life into the world of building management with qualified products and solutions. SAUTER CASE Suite is a software package for handling building automation projects. Its comprehensive, tried-and-tested library contains energy-efficient strategies and methods. SAUTER CASE Suite is also highly flexible when it comes to adapting solutions to special circumstances, so that even very unusual customer installations can be efficiently operated in terms of energy.

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 data file. This attack can also be used to 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

SAUTER addressed the reported vulnerability by releasing a Service Release for the new version 3.10 SR1 update for the affected software. The updates are available at the following link:

https://www.sauter-controls.com/en/products-sauter/product-details/pdm/gzs-100-150-case-suite.html

REFERENCES

Vendor website
https://www.sauter-controls.com

Product page
https://www.sauter-controls.com/en/products-sauter/product-details/pdm/gzs-100-150-case-suite.html

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

CVE-ID: CVE-2018-17912
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17912

ICS-CERT ICSA-18-305-04
https://ics-cert.us-cert.gov/advisories/ICSA-18-305-04

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/AmznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd
-----END PGP PUBLIC KEY BLOCK-----
```