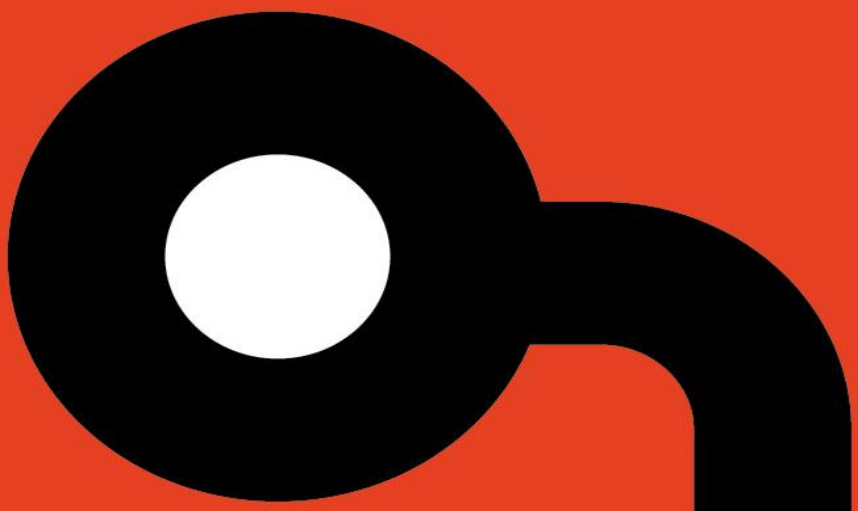
Applied Risk

AR2018004

Schweitzer Engineering Laboratories Compass 3.0.5.1 Insecure File Permissions Privilege Escalation Vulnerability

Author: Gjoko Krstic

Release Date: July 10, 2018



Copyright Notices

OVERVIEW

An insecure file permission was discovered in the Schweitzer Engineering Laboratories (SEL) Compass application with version 3.0.5.1 used for digital content management and file download organization. There are no known public exploits that target these vulnerabilities.

AFFECTED PRODUCTS

Compass;

The following versions are affected:

- SEL Compass 3.0.5.1

The vulnerability has been discovered and validated in Compass 3.0.5.1. Older versions are probably affected too.

IMPACT

SEL Compass suffers from an elevation of privileges vulnerability which can be used by an authenticated user that can change the executable file with a binary of choice and escalate privileges and further infect the affected system.

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. SEL Compass provides simple and convenient tools for managing your SEL digital content. You can use it to keep SEL software applications and relay configuration drivers up to date without manually browsing all the needed product webpages.

VULNERABILITY DETAILS

Insecure File Permissions Privilege Escalation

The application suffers from a privilege escalation vulnerability due to weak or insecure permissions on the entire SEL Compass directory making it world-writable. The vulnerability exists due to the improper permissions on the SEL Compass directory, with the 'F' flag (Full) for 'Everyone' group.

This gives an authenticated attacker the ability to modify or overwrite any file in the Compass directory with malicious code (trojan or a rootkit). This could result in escalation of privileges or malicious effects on the system the next time that a privileged user runs Compass.

Proof of Concept (PoC):

```
C:\Program Files\SEL\SEL Compass>cacls SELCompass.exe
C:\Program Files\SEL\SEL Compass\SELCompass.exe Everyone:(ID)F
                                  NT AUTHORITY\SYSTEM:(ID)F
                                  BUILTIN\Administrators:(ID)F
                                  BUILTIN\Users:(ID)R

---

C:\Program Files\SEL\SEL Compass>cacls * |findstr Everyone
C:\Program Files\SEL\SEL Compass\AccessDatabaseEngine2016.msi Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\compass.ico Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\compass_unavailable copy.ico Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\Compass_Update.ico Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\gdiplus.dll Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\pacparser.dll Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\pacparser.exe Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\SELCompass.exe Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\SEL_Compass.chm Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\uninstall.exe Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\vcredist2010_x64.exe Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\vcredist2010_x86.exe Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\vcredist2015_x64.exe Everyone:(ID)F
C:\Program Files\SEL\SEL Compass\vcredist2015_x86.exe Everyone:(ID)F

C:\Program Files\SEL\SEL Compass>
```

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:L/UI:R/S:C/C:H/I:H/A:H.

MITIGATION

Schweitzer Engineering Laboratories addressed the reported vulnerability by releasing a new updated version: 3.0.6.1 for the affected software. The updates are available at the following link:

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

REFERENCES

Vendor website
http://www.selinc.com

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

Common Weakness Enumeration (CWE) definition 276
https://cwe.mitre.org/data/definitions/276.html
CVE ID: CVE-2018-10604:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10604

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-----
```