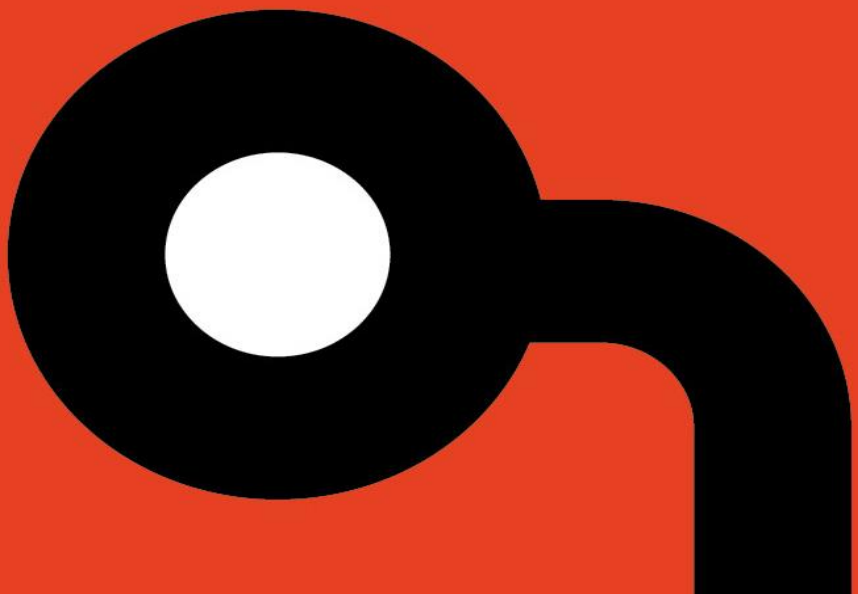
Applied Risk

AR2018006

Siemens SCALANCE S602, S612, S623, S627-2M Reflected Cross-Site-Scripting Vulnerabilities

Author: Nelson Berg

Release Date: November 14, 2018



Copyright Notice

OVERVIEW

A reflected Cross-Site-Scripting vulnerability has been discovered in the Siemens S602, S612, S623, S627-2M SCALANCE devices. There are no known public exploits targeting this vulnerability in said solution.

AFFECTED PRODUCTS

The Siemens S602, S612, S623, S627-2M SCALANCE devices with a software version prior to version V4.0.1.1 are affected.

IMPACT

The integrated web server allows a Cross-Site Scripting (XSS) attack if an administrator is misled into accessing a malicious link. User interaction is required for a successful exploitation. The administrator must be logged into the web interface in order for the exploitation to succeed. Successful exploitation may lead to the ability to bypass critical security measures provided by the firewall.

BACKGROUND

The SCALANCE S firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways.

VULNERABILITY DETAILS

Reflected Cross-Site Scripting (XSS)

The mentioned Siemens firewalls suffer from a reflected Cross-Site Scripting vulnerability. This allows an attacker to craft a malicious link, that when clicked by a logged-in administrator, can allow the attacker to execute commands on the administrator's behalf.

Applied Risk has calculated a CVSSv3 score of 8.2 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:L/E:P/RL:O/RC:C

The vendor's security advisory and CVSS vector string regarding this specific vulnerability can be found in the references.

MITIGATION

Siemens addressed the reported vulnerability by releasing a software update (V4.0.1.1), which can be found in the references.

REFERENCES

Vendor website
https://www.siemens.com/

Vendor's security advisory regarding this vulnerability
https://cert-portal.siemens.com/productcert/pdf/ssa-242982.pdf

Software update V4.0.1.1
https://support.industry.siemens.com/cs/ document/109477325/-delivery-release-anddownload-of-firmware-update-v4-0-1-1-forscalance-s?dti=0&lc=en-WW

Product pages

SCALANCE S602
https://support.industry.siemens.com/cs/products/6gk5602-0ba10-2aa3/scalance-s602?pid=393492&mlfb=6GK5602-0BA10-2AA3&mfn=ps&lc=en-US

SCALANCE S612
https://support.industry.siemens.com/cs/products/6gk5612-0ba10-2aa3/scalance-s612?pid=334322&mlfb=6GK5612-0BA10-2AA3&mfn=ps&lc=en-US

SCALANCE S623
https://support.industry.siemens.com/cs/products/6gk5623-0ba10-2aa3/scalance-s623?pid=17207&mlfb=6GK5623-0BA10-2AA3&mfn=ps&lc=en-US

SCALANCE S627-2M
https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK5627-2BA10-2AA3

OWASP
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

Common Weakness Enumeration (CWE) definition 79
https://cwe.mitre.org/data/definitions/79.html

CVE-ID: CVE-2018-16555
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16555

ICS-CERT ICSA-18-317-04
https://ics-cert.us-cert.gov/advisories/ICSA-18-317-04

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/AmnznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd
-----END PGP PUBLIC KEY BLOCK-----
```