SEC Consult SA-20211104-0 :: Reflected cross-site scripting vulnerability in IBM Sterling B2B Integrator

From: "Functional Account, SEC Consult Vulnerability Lab" <security-research () sec-consult com>
Date: Thu, 4 Nov 2021 09:30:21 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20211104-0 >
=======================================================================
              title: Reflected cross-site scripting vulnerability
            product: IBM Sterling B2B Integrator
 vulnerable version: 5.2.0.0 - 5.2.6.5_3
                     6.0.0.0 - 6.0.3.4
                     6.1.0.0 - 6.1.0.2
      fixed version: 5.2.6.5_4 or higher
                     6.0.3.5 or higher
                     6.1.0.3 or higher
         CVE number: CVE-2021-20562
             impact: medium
           homepage: https://www.ibm.com/products/b2b-integrator
              found: 2021-02-03
                 by: Sutthiwat Panithansuwan (Office Bangkok)
                     Thongchai Silpavarangkura
                     SEC Consult Vulnerability Lab

                     An integrated part of SEC Consult, an Atos company
                     Europe | Asia | North America

                     https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"IBM® Sterling B2B Integrator helps companies integrate all their complex B2B
and EDI processes across partner communities in a single gateway. It provides a
flexible platform, available on premises or through hybrid cloud, that supports
data transformation and most communication protocols; secures your B2B network
and data; provides certified container support; and achieves high availability
for operations with IBM Sterling Global Mailbox. B2B Integrator enables you to
reduce costs by consolidating on a single platform and automating B2B processes
across enterprises, while providing governance, adherence to standards and
visibility for those processes."

Source: https://www.ibm.com/products/b2b-integrator


Business recommendation:
------------------------
SEC Consult recommends updating to the latest version of IBM Sterling B2B
Integrator.

An in-depth security analysis performed by security professionals is highly
advised, as the software may be affected from further security issues.


Vulnerability overview/description:
-----------------------------------
1) Reflected Cross-Site Scripting (CVE-2021-20562)
A reflected cross-site scripting vulnerability has been identified across
multiple functions in the mailbox component of IBM Sterling B2B Integrator,
which can be exploited under the specific condition of a victim's session.


Proof of concept:
-----------------
1) Reflected Cross-Site Scripting (CVE-2021-20562)
The "securetoken" parameter of the following scripts is affected by the
reflected cross-site scripting vulnerability:
/mailbox/jsp/MBIList.jsp
/mailbox/jsp/MBISearch.jsp
/mailbox/jsp/MBISend.jsp

The exploitation is successful if the "SCI_DLSSO" cookie is valid, and the
"JSESSIONID" cookie of the mailbox is invalid or does not exist. One of the
possible scenarios to meet this condition is proceeding to the following steps:

1. Log in to the dashboard via https://<host>/dashboard/Login to obtain an
"SCI_DLSSO" cookie.

2. Visit the mailbox web page via https://<host>/mailbox, which gets logged
in automatically since the web browser sends the "SCI_DLSSO" cookie from the
step 1 to obtain a "JSESSIONID" cookie of the mailbox (Path=/mailbox/).

3. Log out of the dashboard via https://<host>/dashboard/Logout
The server appears to invalidate both "SCI_DLSSO" cookie in the step 1 and
mailbox's "JSESSIONID" cookie in the step 2.

4. Log in to the dashboard via https://<host>/dashboard/Login again to obtain
a new "SCI_DLSSO" cookie.

5. Visit one of the following attacker-prepared URLs, where the web browser
uses the mailbox's "JSESSIONID" cookie in the step 2 and the "SCI_DLSSO"
cookie in the step 4, as follows:

https://<host>/mailbox/jsp/MBIList.jsp?
securetoken=%3C/script%3E%3Cscript%3Ealert(location.origin);%3C/script%3E%3Cscript%3E
https://<host>/mailbox/jsp/MBISearch.jsp?securetoken=%27%22)%3C/a%3E%3Csvg/onload%3dalert(location.origin)%3E
https://<host>/mailbox/jsp/MBISend.jsp?securetoken=%27)%22%3E%3Csvg/onload=alert(location.origin)%3E


Vulnerable / tested versions:
-----------------------------
The version 6.1.0.0 has been tested. According to the vendor, the following product
versions are affected:
* 5.2.0.0 - 5.2.6.5_3
* 6.0.0.0 - 6.0.3.4
* 6.1.0.0 - 6.1.0.2


Vendor contact timeline:
------------------------
2021-02-06: Contacting vendor through HackerOne
2021-02-07: HackerOne: Report is currently under investigation
2021-02-23: Vendor: still investigating the vulnerability
2021-02-24: Status change to "triaged", confirmed that it is a valid vulnerability
            Kindly asking vendor to keep us informed
2021-03-29: Asking for a status update
```

2021-03-29: Vendor will contact us when the public notice / patch is available
2021-04-16: Vendor is still working on the issue.
2021-06-23: Asking for a status update
2021-06-29: Vendor is still working on the issue.
2021-07-27: Vendor: The issue is fixed in previous releases but not in 6.0 yet,
            which is scheduled for a later date.
2021-10-15: Vendor: all patches are publicly available
2021-11-04: Coordinated release of the security advisory

Solution:

The vendor provides patches for the affected product versions:
* 5.2.6.5_4 or higher
* 6.0.3.5 or higher
* 6.1.0.3 or higher

Further information can be found here:
https://www.ibm.com/support/pages/node/6475301

Workaround:

None

Advisory URL:
----
https://sec-consult.com/vulnerability-lab/

~~~~~~

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an
Atos company. It ensures the continued knowledge gain of SEC Consult in the
field of network and application security to stay ahead of the attacker. The
SEC Consult Vulnerability Lab supports high-quality penetration testing and
the evaluation of new offensive and defensive technologies for our customers.
Hence our customers obtain the most current information about vulnerabilities
and valid recommendation about the risk profile of new technologies.

~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://sec-consult.com/career/

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://sec-consult.com/contact/
~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF Thongchai Silpavarangkura, Sutthiwat Panithansuwan / @2021

By Date By Thread

Current thread:

SEC Consult SA-20211104-0 :: Reflected cross-site scripting vulnerability in IBM Sterling B2B Integrator ***Functional Account, SEC Consult Vulnerability Lab (Nov 04)***
~~~~~~