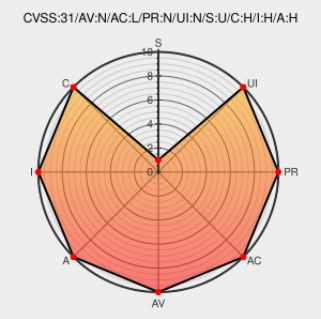
CVE-2021-26295

Published on: 03/22/2021 12:00:00 AM UTC

Last Modified on: 09/16/2021 03:44:00 PM UTC

CVE-2021-26295 - advisory for OFBIZ-12167

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ofbiz from Apache contain the following vulnerability:

Apache OFBiz has unsafe deserialization prior to 17.12.06. An unauthenticated attacker can use this vulnerability to successfully take over Apache OFBiz.

CVE-2021-26295 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache OFBiz** version **17.12.01 to 17.12.05**

Vulnerability Patch/Work Around

Upgrade to at least 17.12.06 or apply the patch at https://github.com/apache/ofbiz-framework/commit/af9ed4e/

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-notifications] 20210324 [jira] [Commented] (OFBIZ-12167) Adds a blacklist (to be serialisation (CVE-2021-26295)
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-notifications] 20210329 [jira] [Commented] (OFBIZ-12167) Adds a blacklist (to be serialisation (CVE-2021-26295)
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-dev] 20210325 Comment out the SOAP and HTTP engines?
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-notifications] 20210329 [jira] [Commented] (OFBIZ-6942) Comment out RMI relate deserialization issue [CVE-2016-2170]
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-commits] 20210427 [ofbiz-site] branch master updated: Updates security page for in 17.12.07
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-notifications] 20210427 [jira] [Updated] (OFBIZ-12212) Comment out the SOAP a 30128]
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-commits] 20210811 [ofbiz-site] branch master updated: Updates security page for
Pony Mail!	lists.apache.org text/html	MISC lists.apache.org/thread.html/r3c1802eaf34aa78a61b4e8e044c214bc94accbd28a11f3a276586a31
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-notifications] 20210605 [jira] [Updated] (OFBIZ-12212) Comment out the SOAP a 30128]
Apache OFBiz SOAP Java Deserialization ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162104/Apache-OFBiz-SOAP-Java-Deserialization.html
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-dev] 20210325 Re: Comment out the SOAP and HTTP engines?
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-dev] 20210329 Re: Comment out the SOAP and HTTP engines?
Pony Mail!	lists.apache.org text/html	MLIST [ofbiz-notifications] 20210729 [jira] [Updated] (OFBIZ-12212) Comment out the SOAP a 30128]

Related QID Numbers

375399 Apache OFBiz Unsafe Deserialization Vulnerability (OFBIZ-12167)

Exploit/POC from Github

CVE-2021-26295-POC 利用DNSlog进行CVE-2021-26295的漏洞验证。 使用 poc：将目标放于target.txt后运行python poc.py即可。（Jdk环境需<12，否则ysoserial无法正常…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Ofbiz	All	All	All	All

cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*:

Discovery Credit

Apache OFBiz would like to thank the first report from "r00t4dm at Cloud-Penetrating Arrow Lab and Longofo at Knownsec 404 Team" and the second report by MagicZero from SGLAB of Legendsec at Qi'anxin Group.

Social Mentions

Source	Title	Posted (UTC)
@GrupoICA_Ciber	?APACHE? Múltiples vulnerabilidades de severidad alta en productos APACHE: CVE-2021-26295,CVE-2020-13949 Más inf… twitter.com/i/web/status/1…	2021-03-27 08:55:22
@GrupoICA_Ciber	?APACHE? Múltiples vulnerabilidades de severidad alta en productos APACHE: CVE-2021-26295,CVE-2020-13936 Más inf… twitter.com/i/web/status/1…	2021-03-30 07:55:18
@goby77463399	New vulnerability: Apache OFBiz rmi RCE (CVE-2021-26295) More Vulnerabilities, github.com/gobysec/GobyVu… Provide Feed… twitter.com/i/web/status/1…	2021-04-01 06:45:40
@3XS0	New vulnerability: Apache OFBiz rmi RCE (CVE-2021-26295) More Vulnerabilities, github.com/gobysec/GobyVu… Provide Feed… twitter.com/i/web/status/1…	2021-04-02 11:22:13
@zhzyker	#CVE CVE-2021-26295 Apache OFBiz RCE RMI Deserializes Remote Code Execution ROME chain provided by ysoserial make d… twitter.com/i/web/status/1…	2021-04-04 08:22:23
@zhzyker	脚本在这里： github.com/zhzyker/exphub…	2021-04-04 09:21:37
@ipssignatures	The vuln CVE-2021-26295 has a tweet created 0 days ago and retweeted 10 times. twitter.com/zhzyker/status… #pow1rtrtwwcve	2021-04-04 15:06:00
@GrupoICA_Ciber	?APACHE? Múltiples vulnerabilidades de severidad alta en productos APACHE: CVE-2021-26295,CVE-2021-26919 Más inf… twitter.com/i/web/status/1…	2021-04-07 07:55:03
@ka0com	Apache OFBizの脆弱性 (CVE-2021-26295) の検証：環境構築編 - nekotosec.com/verification-o…	2021-04-14 09:12:43
@ipssignatures	It's new to me that WatchGuard has a protection/signature/rule for the vulnerability CVE-2021-26295.… twitter.com/i/web/status/1…	2021-04-27 19:02:03
@ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2021-26295. #S75xmcp23zv446	2021-04-27 19:02:03
@ipssignatures	It's new to me that CheckPoint has a protection/signature/rule for the vulnerability CVE-2021-26295.… twitter.com/i/web/status/1…	2021-04-29 11:02:01
@ipssignatures	I know one more IPS that has a protection/signature/rule for the vulnerability CVE-2021-26295. ipssignatures.appspot.com/?cve=CVE-2021-… #S75xmcp23zv446	2021-04-29 11:02:01
@wallcorners	Phân tích CVE-2021-26295 Apache OFBIZ codechay.com/tin-tuc-chung-…	2021-06-19 19:21:01
@RapidSafeguard	Apace Ofbiz RCE | CVE-2021-26295 youtu.be/2vpv8zUnmhI @vulnmachines #infosec #cybersecurity #bugbounty	2021-06-20 18:47:58
@Securityblog	apache ofbiz rce | cve-2021-26295 poc youtu.be/2vpv8zUnmhI via @YouTube	2021-06-24 12:34:36

@d34dr4bbit	Watch "apache ofbiz rce | cve-2021-26295 poc" on YouTube aeternusmalus.wordpress.com/2021/06/24/wat…	2021-06-24 12:34:58
@Securityblog	apache ofbiz rce | cve-2021-26295 poc youtu.be/2vpv8zUnmhI via @YouTube	2021-08-08 15:35:17
@ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2021-26295.… twitter.com/i/web/status/1…	2021-09-13 08:02:04
@ipssignatures	I know 2 other IPSs that have protections/signatures/rules for the vulnerability CVE-2021-26295. ipssignatures.appspot.com/?cve=CVE-2021-… #S75xmcp23zv446	2021-09-13 08:02:04
@ipssignatures	It's new to me that Astaro has a protection/signature/rule for the vulnerability CVE-2021-26295.… twitter.com/i/web/status/1…	2023-03-19 04:02:01
@ipssignatures	I know 3 other IPSs that have protections/signatures/rules for the vulnerability CVE-2021-26295. ipssignatures.appspot.com/?cve=CVE-2021-… #S75xmcp23zv446	2023-03-19 04:02:01

← Previous ID

Next ID→