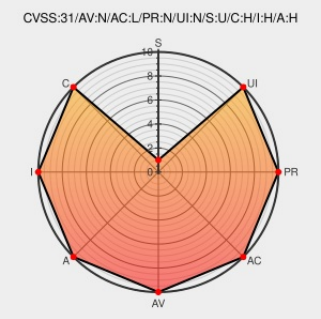
CVE-2020-7961

Published on: 03/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7961

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



Certain versions of Liferay Portal from Liferay contain the following vulnerability:

Deserialization of Untrusted Data in Liferay Portal prior to 7.2.1 CE GA2 allows remote attackers to execute arbitrary code via JSON web services (JSONWS).

CVE-2020-7961 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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
Known Vulnerabilities	Vendor Advisory, portal.liferay.dev, text/html	MISC portal.liferay.dev/learn/security/known-vulnerabilities
Liferay Portal Java Unmarshalling Remote Code	Third Party Advisory	MISC packetstormsecurity.com/files/157254/Liferay-

Execution ≈ Packet Storm	VDB Entry packetstormsecurity.com text/html	Portal-Java-Unmarshalling-Remote-Code-Execution.html
FreakOut – Leveraging Newest Vulnerabilities for creating a Botnet - Check Point Research	Exploit Third Party Advisory research.checkpoint.com text/html	MISC research.checkpoint.com/2021/freakout-leveraging-newest-vulnerabilities-for-creating-a-botnet/
Liferay Portal Remote Code Execution ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158392/Liferay-Portal-Remote-Code-Execution.html
CST-7205 Unauthenticated Remote code execution via JSONWS	Vendor Advisory portal.liferay.dev text/html	CONFIRM portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/117954271

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Liferay Portal	All	All	All	All

cpe:2.3:a:liferay:liferay_portal:*:*:*:*:community:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@papa_anniekey	これとは別で、殆ど注目されていませんが、Liferay Portalに対するDeserializedの脆弱性（CVE-2020-7961）を突く攻撃（Unauth + RCE)も広く観測しています。こちらも簡単に刺さるので注意です。	2021-04-06 23:05:47
@NeobeePaul	synacktiv.com/en/publication…	2021-04-07 01:02:23
@ipssignatures	It's new to me that McAfee has a protection/signature/rule for the vulnerability CVE-2020-7961.… twitter.com/i/web/status/1…	2021-06-16 07:02:02
@ipssignatures	I know 6 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-7961. ipssignatures.appspot.com/?cve=CVE-2020-… #Sn4xpm7pmjmzqu	2021-06-16 07:02:02
@devesh2003	@stokfredrik synacktiv.com/en/publication…	2021-07-09 04:50:20
@buaqbot	Liferay Portal CE 反序列化命令执行漏洞（CVE-2020-7961） ift.tt/3Dfaxzd ift.tt/2WpMPjd	2021-08-25 05:11:15
@hiramcoop	Liferay en su versión 7.1.10, tiene la vulnerabilidad CVE-2020-7961, usada por el malware Kinsing para inyectar min… twitter.com/i/web/status/1…	2021-09-21 20:28:08

@AttilaDeak01	2/2 CVE-2021-38647,3 CVE-2020-28188,2 CVE-2017-9805,1 CVE-2019-12725,1 CVE-2020-7961,1	2021-10-02 18:11:58
@th3_protoCOL	Threat Actor leveraging open source tools to target Liferay Portals via CVE-2020-7961 ⚠ Exploit:… twitter.com/i/web/status/1…	2021-10-04 17:56:36
@th3_protoCOL	I wonder if @GreyNoiseIO has tags for CVE-2020-7961 scanning ? https://t.co/bG2vGYm6sj	2021-10-04 19:02:28
@chybeta	; + CVE-2020-7961 = RCE https://t.co/AFMwrIuaPh	2021-11-28 15:32:29
@Har_sia	CVE-2020-7961 har-sia.info/CVE-2020-7961.… #HarsiaInfo	2021-11-29 23:00:04
@Arkbird_SOLG	The Ukrainian IP is also active for exploit the CVE-2020-7961 vulnerability and deploy Kinsing implant. This uses… twitter.com/i/web/status/1…	2021-12-10 21:53:57
@TekDefense	For those that don't have yara rules in VT for this stuff, this VT query will help you get an initial thread to pull: tag:cve-2020-7961	2022-10-04 14:15:07

← Previous ID

Next ID→