



CVE-2020-28885

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-28885
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-28 12:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	** DISPUTED ** Liferay Portal Server tested on 7.3.5 GA6, 7.2.0 GA1 is affected by OS Command Injection. An administrator can execute arbitrary OS commands by sending a specially crafted request to the Liferay Portal Server. The vulnerability is due to the Liferay Portal Server not properly sanitizing user input before passing it to the operating system. An attacker can exploit this vulnerability by sending a request with a specially crafted payload that contains a command to be executed on the server. The attacker can then execute arbitrary OS commands on the server, which could lead to a complete compromise of the system.

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Liferay Portal	7.2	ga1	All	All
Application	Liferay	Liferay Portal	7.3.5	ga6	All	All

References

Reference	Source	Link	Tags
Some way to execute OS command in Liferay Portal by TPDanh Medium		medium.com	
Some way to execute OS command in Liferay Portal by TPDanh Medium	MISC	medium.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report