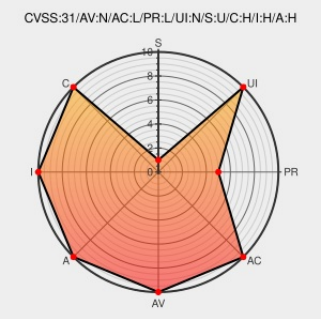
CVE-2020-13445

Published on: 06/10/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-13445

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



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

In Liferay Portal before 7.3.2 and Liferay DXP 7.0 before fix pack 92, 7.1 before fix pack 18, and 7.2 before fix pack 6, the template API does not restrict user access to sensitive objects, which allows remote authenticated users to execute arbitrary code via crafted FreeMarker and Velocity templates.

CVE-2020-13445 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[LPE-17023] Remote code execution (RCE) with FreeMarker/Velocity templates - Liferay Issues	Patch Vendor Advisory issues.liferay.com	MISC issues.liferay.com/browse/LPE-17023

	text/html	
GHSL-2020-043: Server-side template injection in Liferay - CVE-2020-13445 - GitHub Security Lab	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC securitylab.github.com/advisories/GHSL-2020-043-liferay_ce
CST-7302 Remote code execution with FreeMarker/Velocity templates (CVE-2020-13445)	Patch Vendor Advisory portal.liferay.dev text/html	CONFIRM portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/119317411

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	7.1	ga1	All	All
Application	Liferay	Liferay Portal	7.1	ga2	All	All
Application	Liferay	Liferay Portal	7.1	ga3	All	All
Application	Liferay	Liferay Portal	7.1.1	ga2	All	All
Application	Liferay	Liferay Portal	7.2	ga1	All	All
Application	Liferay	Liferay Portal	7.3	ga1	All	All
Application	Liferay	Liferay Portal	7.3	ga2	All	All
Application	Liferay	Liferay Portal	7.1	ga1	All	All
Application	Liferay	Liferay Portal	7.1	ga2	All	All
Application	Liferay	Liferay Portal	7.1	ga3	All	All
Application	Liferay	Liferay Portal	7.1.1	ga2	All	All
Application	Liferay	Liferay Portal	7.2	ga1	All	All
Application	Liferay	Liferay Portal	7.3	ga1	All	All
Application	Liferay	Liferay Portal	7.3	ga2	All	All

cpe:2.3:a:liferay:liferay_portal:7.1:ga1:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.1:ga2:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.1:ga3:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.1.1:ga2:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.2:ga1:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.3:ga1:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.3:ga2:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.1:ga1:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.1:ga2:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.1:ga3:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.1.1:ga2:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.2:ga1:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.3:ga1:*:*:community:*:*:*:

cpe:2.3:a:liferay:liferay_portal:7.3:ga2:*:*:community:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→