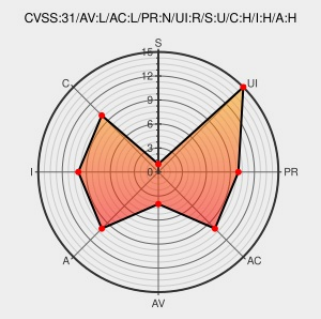
CVE-2020-13771

Published on: 11/12/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-13771

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



Certain versions of Endpoint Manager from Ivanti contain the following vulnerability:

Various components in Ivanti Endpoint Manager through 2020.1.1 rely on Windows search order when loading a (nonexistent) library file, allowing (under certain conditions) one to gain code execution (and elevation of privileges to the level of privilege held by the vulnerable component such as NT AUTHORITY\SYSTEM) via DLL hijacking. This affects ldiscn32.exe, IpmiRedirectionService.exe, LDAPWhoAmI.exe, and ldprofile.exe.

CVE-2020-13771 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Advisory CVE-2020-13771 - Ivanti Unified Endpoint Manager DLL search order hijacking privilege escalation | JUMPSEC LABS	Third Party Advisory labs.jumpsec.com	MISC labs.jumpsec.com/advisory-cve-2020-13771-ivanti-uem-dll-

text/html hijacking/

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	Ivanti	Endpoint Manager	All	All	All	All

cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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