CVE-2019-12377

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-12377
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-03 20:29:00 UTC
Updated	2019-06-04 16:31:00 UTC
Description	A vulnerable upl/async_upload.asp web API endpoint in Ivanti LANDESK Management Suite (LDMS, aka Endpoint Manage

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ivanti	Landesk Management Suite	10.0.1.168	service_update_5	All	All
Application	Ivanti	Landesk Management Suite	10.0.1.168	service_update_5	All	All

References

Reference	Source	Link	Tags
LANDesk Management Server - Multiple Vulnerabilities - GNZ Labs	MISC	www.gnzlabs.io	Third Party Advisory
www.gnzlabs.io/gnzlabs-blog/landesk-management-server-arbitrary-file-upload	MISC	www.gnzlabs.io	Exploit, Third Party Advisory
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.

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