hello@jumpsec.com

0333 939 8080

Vendor page: www.ivanti.com
CVE Reference: CVE-2020-13772
Published: 13/11/2020
CVSS 3.1 Score: 5.3 – AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Attack Vector: Remote, unauthenticated
Credits: Andrei Constantin Scutariu, Lenk Ratchakrit, Calvin Yau

Summary

Ivanti Unified Endpoint Manager's "ldcient" component expose information about the system that could be used in further attacks against the system.

Mitigation

There is currently no fix for this issue. The vendor has yet to release a patch to address the vulnerability; it is advised to review the host configuration and monitor for suspicious activity. If possible, consider disabling or whitelisting access to the affected URLs.

Technical details

The following endpoint expose information about the system, such as environment variables, domain name, internal paths and CPU information:

- /ldclient/ldprov.cgi, HTTP 9595
- /ldclient/ldprov.cgi, HTTPS 9594
- /ldclient/ldprov.cgi, HTTPS 9593

Timeline

15/04/2020: Issue reported to the vendor
16/04/2020: Vendor acknowledged the issues
02/06/2020: CVE number assigned from MITRE
13/07/2020: 90 days notice period for disclosure given to the vendor
13/11/2020: Advisory published by JUMPSEC

Disclaimer

[Categories]

Application Security

Binary Analysis

burpsuite

CTFs

Detection

Exploitation

Forensics

Incident Response

Jumpsec

Monitoring

network

Network Forensics

Network Tools

Obfuscation

Password Cracking

Pcap analysis

Research

Security Bug

Social Engineering

Uncategorized

Vulnerability

Windows

GitHub Activity

Follow JUMPSECLabs

Latest from JUMPSEC

2023 Cyber Security Predictions

NCSC Annual Review 2022

Combining Artificial Intelligence with Threat Intelligence

Building Sustainable Services

Disclaimer

Software: Mutiny Network Monitoring Appliance Affected versions: <= 7.2.0-10855 Vendor page: www.mutiny.com CVE Reference: CVE-2022-37832 Published: 16/12/2022 CVSS 3.1 Score:...

When designing and implementing a machine learning model, ensuring it is continually updated is a challenge that all engineers encounter. In this article, I explore the...

Implementation and Dynamic Generation for Tasks in Apache Airflow

I recently worked on a project focused on log anomaly detection using manageable machine learning pipelines. The pipelines mainly include data collection --- feature extraction...

Jumpsec, Unit 3E - 3F, 33 - 34 Westpoint,
Warple Way, Acton
W3 0RG

To learn more about JUMPSEC's services please get in touch:

Give us a call: 0333 939 8080

Send us a message: hello@jumpsec.com

To learn more about JUMPSEC'S services please get in touch:

Give us a call: 0333 939 8080

Send us a message: hello@jumpsec.com

Jumpsec, Unit 3E - 3F, 33 - 34 Westpoint,
Warple Way, Acton, W3 0RG