hello@jumpsec.com

0333 939 8080

Vendor page: www.ivanti.com
CVE Reference: CVE-2020-13769
Published: 13/11/2020
CVSS 3.1 Score: 7.4 - AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
Attack Vector: Remote, authenticated
Credits: Andrei Constantin Scutariu, Lenk Ratchakrit, Calvin Yau

Summary

A number of web components in Endpoint Manager do not properly sanitize user input when executing SQL queries, leaving the application vulnerable to injection attacks towards the underlying database.
On a standard installation with default options, the account used to query the database is database administrator.

Solution

The issue has been successfully resolved by the vendor in version 2020.1.1. Customers can install the latest available software update to fix the vulnerability. The vendor also reported this has also been fixed in version 2019.1.4, although this has not been verified by JUMPSEC.

Technical details

The following endpoints and parameters are vulnerable and exploitable by any authenticated user:

POST /LDMS/alert_log.aspx?d=alert_log&tb=serverAlertLog.tb
“filterValue” parameter
Type: Stacked, time-based blind, boolean-based blind
Example: filterValue=’;injection_query_here-

POST /remotecontrolauth/api/device
“global”, “displayname”, “ipaddress”, “owner” parameters
Type: Time-based blind, boolean-based blind
Example: “global”:”‘+(injection_query_here)+'”
This instance also requires a valid “sessionid” in the request.

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