CVE-2026-51831 and CVE-2026-51832: Two More Local Privilege Escalation IDrive Vulnerabilities



I've found two additional local privilege-escalation IDrive vulnerabilities in the Windows Backup client.

As with the previous post about this software, we are beginning the public disclosure process to ensure organizations and individuals using IDrive for Windows can respond and patch their systems.



If you're using IDrive Windows Backup, the rest of this post explains what to look for and what you can do now to remediate.

Once again, key technical details will be omitted to give users time to patch before a full proof of concept is made available.

What is IDrive?

IDrive is a privately owned, cloud-based file backup tool company.

Their software is geared toward individuals and small- to medium-sized organizations, with backup clients available for Windows, macOS, and Linux. This is similar to Veeam or Backblaze, which let users back up critical system files and personal data to cloud storage.

These vulnerabilities are specific to the Windows version of their backup client.

Details Regarding the Discovery of these Vulnerabilities

IDrive's Windows client has had a couple of local privilege escalation vulnerabilities over the years, the first of which is tracked in the National Vulnerability Database (NVD) under CVE-2020-15351.

Notably, at the end of 2025 and spanning into 2026, we discovered a new local privilege escalation tracked in the NVD as CVE-2026-1995, which can be read about on our blog.

Essentially, CVE-2026-1995 was a vulnerability in one of the mechanisms by which IDrive would perform inter-process communication.

A graphical interface running in a normal user context would be able to instruct the elevated IDrive service to perform tasks that require full access to the system by creating a specially crafted file that the elevated service would then parse.

This parsed data would be used to trigger relevant backup jobs based on parameters set in the file.

Inter-process communication is normal for any software that requires a delineation between the standard user experience and actions that require elevated permissions.

A logic bug existed that allowed a user to induce unintended behavior and made it possible to run any process on the system with elevated SYSTEM permissions.

IDrive released a patch for their software shortly after the public disclosure of CVE-2026-1995 and requested that I verify the patch was effective.

After reviewing the software, I confirmed the vulnerability was removed.

The remediation involved completely removing this channel for inter-process communication. While this patch was effective, it raised a question: how was the application handling inter-process communication now?

This led me to dive back into the software to determine what other inter-process communication mechanisms existed and to ensure that its operation was secure.

Technical Details for CVE-2026-51831 and CVE-2026-51832

The way that most inter-process communication in IDrive works is through a network service.

The IDrive service opens a port that is only accessible from the local system and listens for network traffic from the graphical interface. This data is then parsed by the service and, based on the data that is sent to the service, the service will perform any number of predetermined actions—such as starting backup jobs or copying backup data to various backup storage providers.

In order to transmit data between processes, some manner of serialization and deserialization of data is necessary to preserve the structure of the data and the specific data types of data in the structure.

Common examples of this include JSON and XML.

In the case of the IDrive service, the manner in which it performed serialization and deserialization was insecure and would allow an attacker to inject arbitrary code into the data being sent to the service.

This code would then be parsed and executed by the deserializer with the service's elevated SYSTEM permissions. ***This specific issue is tracked as CVE-2026-51831.***

Going beyond this, I also assessed the various actions the service could take based on the data that was being sent during normal usage of the application.

One particular feature of the service contained functionality that would spawn a process to perform tasks related to managing mounted file shares on the system. However, this

functionality did not properly sanitize input, which allowed the injection of arbitrary code. ***This specific vulnerability is tracked as CVE-2026-51832.***

Impact

It is important to note that despite the fact these vulnerabilities are triggered through a network service, there is no possible configuration in which this service would be available from remote systems.

This means that exploitation of these vulnerabilities requires at least low-privileged access to a system running a vulnerable version of the software.

That said, ***these vulnerabilities allow for an authenticated user with low-level, restricted access to run executables with full system privileges on a Windows machine.***

This ultimately would allow an attacker to steal sensitive information, modify system configurations, or execute additional malicious code.

Remediation

These IDrive vulnerabilities are remediated **for Windows version 7.0.1.2 and above**.

If you are using IDrive Backup for Windows, we recommend patching to the latest version of the software as soon as possible. The latest version can be downloaded here.

Disclosure Timeline

- 04-28-2026 – IDrive is informed of the discovery of two new, distinct vulnerabilities.
- 04-29-2026 – IDrive acknowledges receipt of the details and states they are beginning to investigate the reported vulnerabilities.
- 05-01-2026 – IDrive confirms reproducibility of the vulnerabilities and that they are beginning to work on a patch.
- 05-07-2026 – FRSecure requests CVE reservations from MITRE for these issues.
- 05-07-2026 – IDrive releases the patched version 7.0.1.2 and requests validation that the vulnerabilities are remediated.
- 05-08-2026 – FRSecure verifies that the patches have successfully remediated the vulnerabilities and notifies IDrive.
- 07-08-2026 – MITRE notifies FRSecure of reservations for CVE-2026-51831 and CVE-2026-51832.
- 09-28-2026 – Public disclosure release timeline finalized.
- 10-28-2026 – Vulnerabilities disclosed.

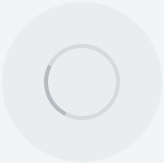


Categories: Labs, Security Breaches, Vulnerability Management • By Matt Owens • October 29, 2026 • Leave a comment

Tags: breaches | cybersecurity | data security | hacking | IDrive | incident response | information security | InfoSec | Windows Backup

Share this post





Author: Matt Owens

Matt is a security researcher and penetration tester at FRSecure. In addition, he works alongside the technical services team to find improvements to existing processes and develop new product offerings. Matt discovered his love for technology and hacking in high school, doing a variety of programming and computer hardware classes. Since then, he has been working in IT and cybersecurity for 9 years across several organizations. He has also received several professional certifications, such as the CompTIA Security+, OSCP, OSEP, OSWE, OSED, OSMR, and OSCE3. Matt is passionate about uncovering security flaws and assisting customers and vendors in remediating any identified flaws to prevent attackers from exploiting weaknesses in their software and systems. He believes that a culture focused on positivity, openness, and a willingness to learn from mistakes leads to the best security outcomes!

PREVIOUS

AI Penetration Testing vs. Human-Led: The Real Results of 13 Tests

Related Posts



AI Penetration Testing vs. Human-Led: The Real Results of 13 Tests

October 22, 2026



Hugging Face AI Incident: Agent Risk and Practical Recommendations

July 31, 2026



CVE-2026-1995: IDrive Windows Backup Vulnerability Discovery

March 23, 2026



Significant Business Email Compromise Payloads: 2025 State of InfoSec Series

October 9, 2025



Token Theft Attacks & MFA Defeat: 2025 State of Infosec Incident Stories

June 2, 2025



2025 State of Infosec: Incident Response Stories and Useful Findings

March 28, 2025

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name*

Email*

Website

Save my name, email, and website in this browser for the next time I comment.

Post comment

Recent Posts



CVE-2026-51831 and CVE-2026-51832: Two More Local Privilege Escalation IDrive Vulnerabilities

October 29, 2026



AI Penetration Testing vs. Human-Led: The Real Results of 13 Tests

October 22, 2026



Hugging Face AI Incident: Agent Risk and Practical Recommendations

July 31, 2026



CMMC Phase 2 Is on Pause. Your Obligation to Secure Federal Data Isn't.

July 15, 2026



CVE-2026-1995: IDrive Windows Backup Vulnerability Discovery

March 23, 2026

Blog Categories

AI & LLMs	(1)
Audit Prep	(15)
C-Suite	(14)
CISSP	(1)
Cloud Security	(2)
Culture	(40)
Cyber Insurance	(10)
Framework Assessments	(20)
Incident Response	(51)
Information Security	(101)
Labs	(16)
Media Appearances	(3)
News	(27)

PCI (5)
Penetration Testing (16)
Personal Security (16)
Risk Assessments (20)
Security Breaches (48)
Security Standards (50)
Social Engineering (22)
Tools (12)
Uncategorized (1)
vCISO (5)
Vendor Risk Management (6)
Vulnerability Management (6)
Vulnerability Scanning (3)

All Policy Templates

Acceptable Use Policy Template

Asset Management Policy Template

Audit Policy Template

Awareness Training and Personnel Security Policy Template

Business Continuity and Disaster Recovery Policy Template

Change Management Policy Template

Encryption Policy Template

IAM Policy Template

Incident Management Template

Information Classification and Management Policy

Information Security Policy Template

Network Management Policy Template

PCI Policy Template

Physical Security Policy Template

Remote Work Policy Template

Risk Management Policy Template

System Development and Procurement Policy Template

Vendor Management Policy Template

Vulnerability Management Policy Template

Information Security Definitions: Appendix A

CONTACT US | 877-756-8298 | SUBSCRIBE

SERVICES

Virtual CISO

Penetration Testing

Incident Response

Risk Assessment

Vulnerability Scanning

Social Engineering

PCI

Gap Assessment

Tabletops

Vendor Risk Management

Purple Team

SOC 2

CMMC

Cloud Security Assessment

OBJECTIVE

Build Your Security Program

Attack Simulation

On-Demand Security Experts

Compliance Preparation

COMPANY

About

Blog

Contact

Careers

Case Studies

Resources

Privacy Policy

Press Kit

© 2026 FRSECURE LLC