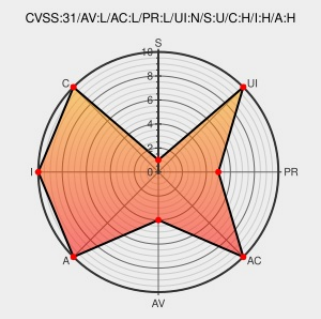
CVE-2021-36665

Published on: Not Yet Published

Last Modified on: 07/20/2022 05:02:00 PM UTC

CVE-2021-36665

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



Certain versions of Insync Client from Druva contain the following vulnerability:

An issue was discovered in Druva 6.9.0 for macOS, allows attackers to gain escalated local privileges via the inSyncUpgradeDaemon.

CVE-2021-36665 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	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Druva | The Data Resiliency Cloud	druva.com text/html	MISC druva.com

Druva inSync for Mac Local Privilege Escalation - Imhotep Is Invisible	imhotepisinvisible.com text/html	MISC imhotepisinvisible.com/druva-lpe/
Security Advisory for inSync Client 7.0.1 and before - Druva Documentation	docs.druva.com text/html	MISC docs.druva.com/Knowledge_Base/Security_Update/Security_Advisory_for_inSync_Client_7.0.1_and

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Druva	Insync Client	All	All	All	All
Application	Druva	Insync Client	All	All	All	All

cpe:2.3:a:druva:insync_client:*:*:*:*:*:macos:*:*:

cpe:2.3:a:druva:insync_client:*:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-36665 : An issue was discovered in Druva 6.9.0 for macOS, allows attackers to gain escalated local privile… twitter.com/i/web/status/1…	2022-07-12 14:06:47
/r/netcve	CVE-2021-36665	2022-07-12 15:39:15

← Previous ID

Next ID→

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