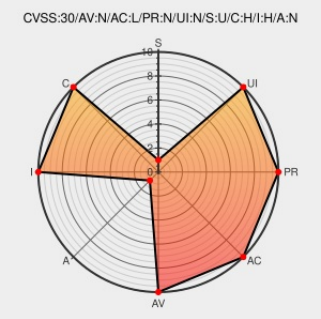
CVE-2019-9565

Published on: 03/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2019-9565

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



Certain versions of Antidote from Druide contain the following vulnerability:

Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.

CVE-2019-9565 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Abusing Unsafe Defaults in Active Directory Domain Services: A	Exploit	MISC secsecure.net/2019/03/30/abusing

Abusing Unsafe Defaults in Active Directory Domain Services: A Real-World Case Study | GoSecure	Exploit Third Party Advisory gosecure.net text/html	MISC gosecure.net/2019/02/20/abusing-unsafe-defaults-in-active-directory/
Security—Improvement to Antidote on Windows | Druide	Vendor Advisory www.druide.com text/html	MISC www.druide.com/en/news/security-improvement-antidote-windows

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Druide	Antidote	All	All	All	All
Application	Druide	Antidote	All	All	All	All

cpe:2.3:a:druide:antidote:*:*:*:*:*:*:*:*:

cpe:2.3:a:druide:antidote:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→