



CVE-2020-15931

Published on: 10/20/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

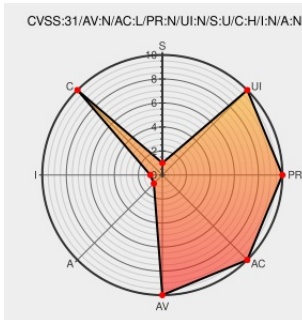
CVE-2020-15931

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Account Lockout Examiner](#) from [Netwrix](#) contain the following vulnerability:

Netwrix Account Lockout Examiner before 5.1 allows remote attackers to capture the Net-NTLMv1/v2 authentication challenge hash of the Domain Administrator (that is configured within the product in its installation state) by generating a single Kerberos Pre-Authentication Failed (ID 4771) event on a Domain Controller.

CVE-2020-15931 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Netwrix Account Lockout Examiner Disclosure Vulnerability	Third Party Advisory www.optiv.com text/html	MISC www.optiv.com/explore-optiv-insights/source-zero/netwrix-account-lockout-examiner-41-disclosure-vulnerability

Netwrix Reports
Vulnerability in
Netwrix Account
Lockout Examiner
4.1

Vendor Advisory

www.netwrix.com

text/html



www.netwrix.com/netwrix_reports_vulnerability_in_netwrix_account_lockout_examiner_4_1.html

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

Exploit/POC from Github

Netwrix Account Lockout Examiner 4.1 Domain Admin Account Credential Disclosure Vulnerability

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netwrix	Account Lockout Examiner	All	All	All	All
Application	Netwrix	Account Lockout Examiner	All	All	All	All
cpe:2.3:a:netwrix:account_lockout_examiner:*.*.*.*.*.*.*.*						
cpe:2.3:a:netwrix:account_lockout_examiner:*.*.*.*.*.*.*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous ID Next ID →		