RhinoSecurityLabs / **CVEs** Public

A collection of proof-of-concept exploit scripts written by the team at Rhino Security Labs for various CVEs.

BSD-3-Clause license

618 stars 202 forks

Star Notifications

Code Issues Pull requests Actions Security Insights

master Go to file

DaveYesland Correct incomplete push, oops fixes #7 ... on May 26 95

View code

README.md

Rhino CVE Proof-of-Concept Exploits

A collection of proof-of-concept exploit scripts written by the team at Rhino Security Labs for various CVEs.

- CVE-2022-25372: Local Privilege Escalation In Pritunl VPN Client
- CVE-2022-25237: Authorization Bypass Leading to RCE in Bonitasoft Web
- CVE-2022-25166: AWS VPN Client Arbitrary File Write as SYSTEM
- CVE-2022-25165: AWS VPN Client Information Disclosure Via UNC Path
- CVE-2021-38112: AWS WorkSpaces Remote Code Execution
- CVE-2020-5377 and CVE-2021-21514: Dell OpenManage Server Administrator Arbitrary File Read
- CVE-2020-13405: MicroWeber Unauthenticated User Database Disclosure
- CVE-2019-9926: LabKey Server CSRF
- CVE-2019-9758: LabKey Server Stored XSS
- CVE-2019-9757: LabKey Server XXE

- CVE-2019-5678: Command Injection in Nvidia GeForce Experience Web Helper
- CVE-2019-5674: NVIDIA GeForce Experience Arbitrary File Overwrites
- CVE-2019-3722: Dell EMC OpenManage Server Administrator (OMSA) XXE
- CVE-2019-16864: CompleteFTP Server Authenticated Remote Command Execution
- CVE-2019-16116: CompleteFTP Server Local Privilege Escalation
- CVE-2019-0227: Apache Axis 1.4 Remote Code Execution
- CVE-2018-8024: Apache Spark XSS vulnerability in UI
- CVE-2018-5758: XXE in Jive-n
- CVE-2018-5757: RCE In AudioCodes 450HD Phone
- CVE-2018-20621: MEmu Android Emulator Local Privilege Escalation
- CVE-2018-1335: Command Injection in Apache Tika-server
- CVE-2018-1000110: User and Node Enumeration Through Jenkins Git Plugin <v3.7
- CVE-2017-7284: Unitrends Force Password Change Without Current Password
- CVE-2017-7283: Unitrends Enterprise Backup Solution RCE via Retore File
- CVE-2017-7282: Unitrends Enterprise Backup Solution LFI
- CVE-2017-7281: Unitrends Enterprise Backup Solution RCE Via File Upload
- CVE-2017-7280: Unitrends Enterprise Backup Solution Command Execution
- CVE-2017-7279: Unitrends Enterprise Backup Server Privilege Escalation.
- CVE-2017-12861: Epson EasyMP Projector Bruteforce PIN
- CVE-2017-12860: Epson EasyMP Projector Hardcoded PIN
- CVE-2016-8972: IBM AIX Bellmail Local Root Exploit
- CVE-2016-6079: AIX lquerylv 5.3, 6.1, 7.1, 7.2 Local Root Exploit
- CVE-2016-3053: AIX lsmcode Local Root Exploit

Releases

No releases published

Packages

No packages published

Contributors 4

DaveYesland Dave Yesland

 **SpenGietz** Spencer Gietzen

 **rhino-hunter-stanton** Hunter Stanton

 **github-actions[bot]**

Languages

Python 75.5% **Shell** 14.9% **HTML** 8.1% **PowerShell** 1.5%