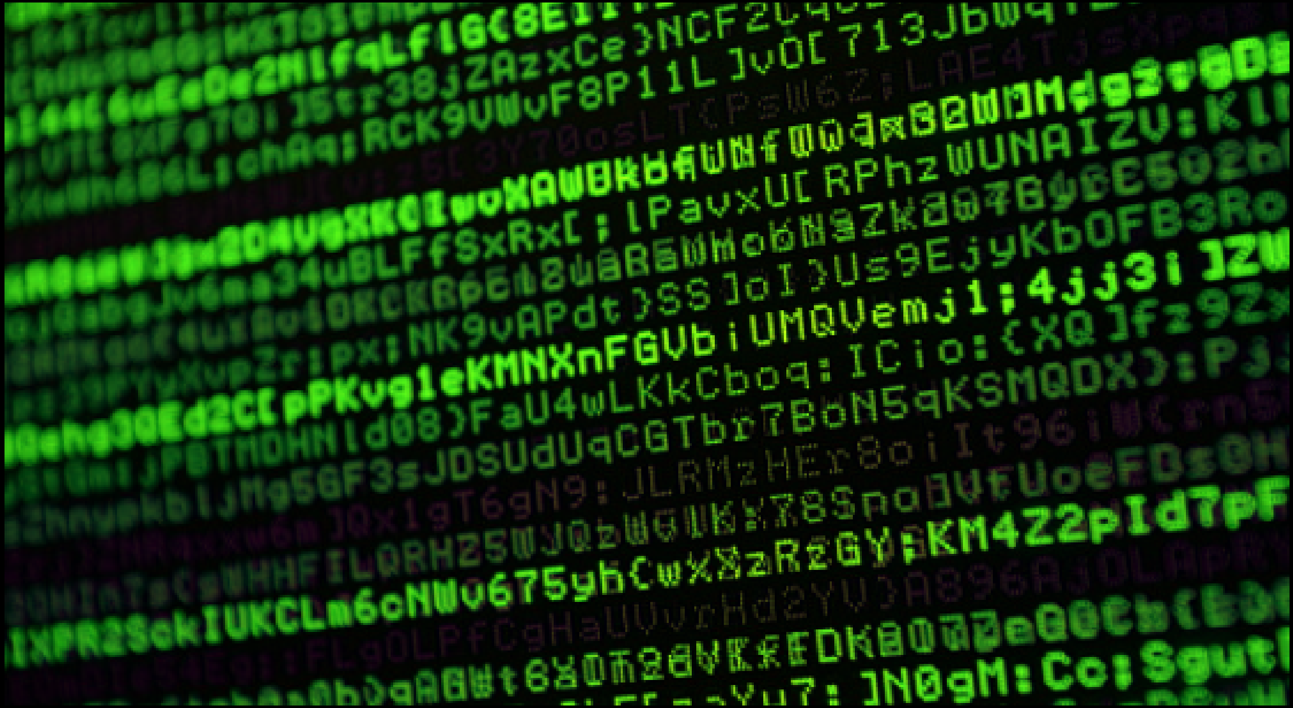
# NAT32 2.2 Build 22284 - Cross-Site Request Forgery

*February 14, 2018*

# ← Exploit Collector



**EDB-ID**: 44034

**Author**: hyp3rlinx

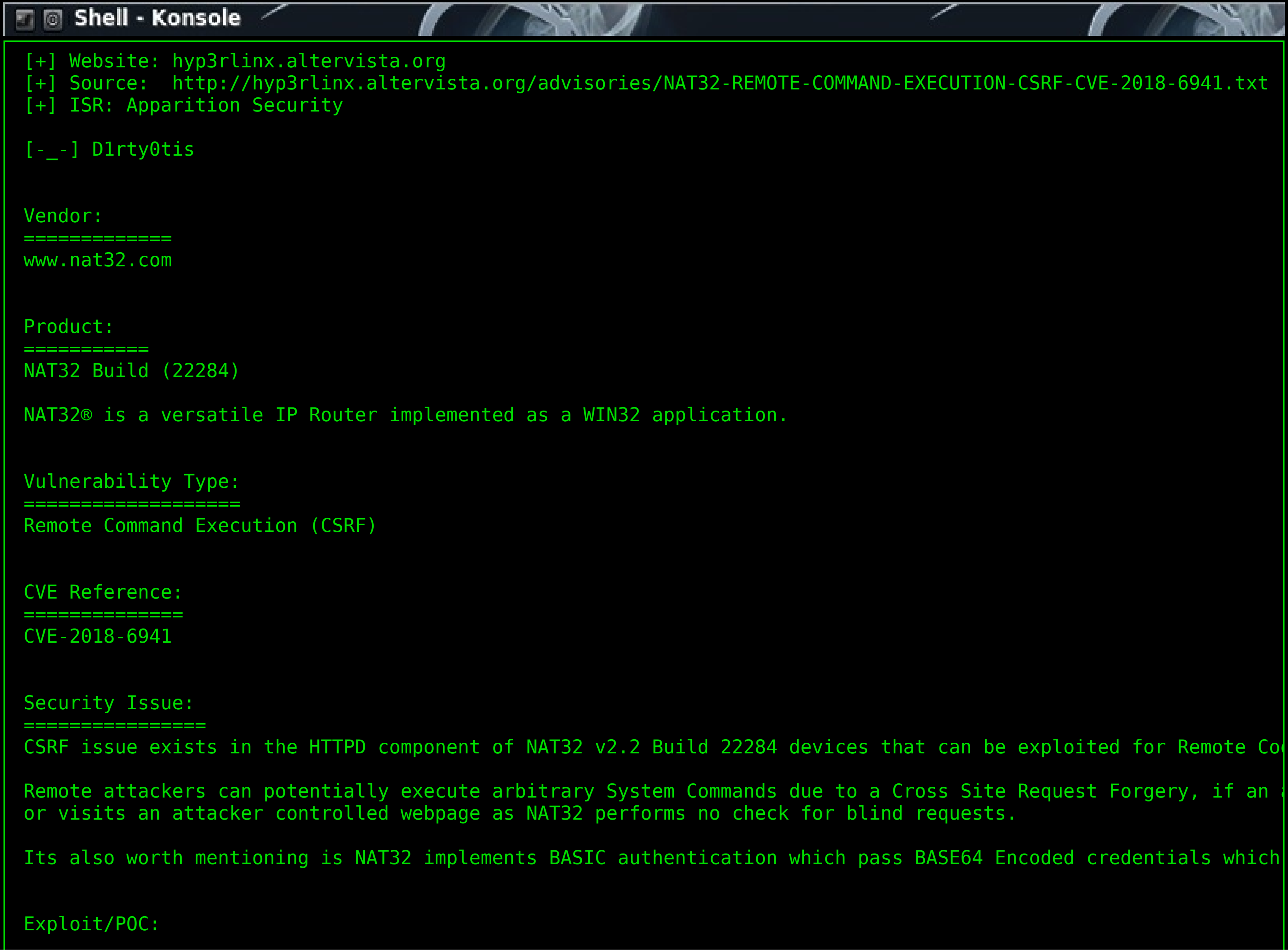
**Published**: **2018-02-14**

**CVE**: CVE-2018-6941

**Type**: Webapps

**Platform**: Windows

# Exploit Collector

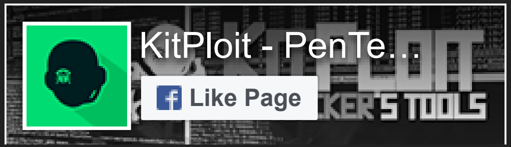


```
[+] Website: hyp3rlinx.altervista.org
[+] Source:  http://hyp3rlinx.altervista.org/advisories/NAT32-REMOTE-COMMAND-EXECUTION-CSRF-CVE-2018-6941.txt
[+] ISR: Apparition Security

[-_-] D1rty0tis


Vendor:
=============
www.nat32.com


Product:
===========
NAT32 Build (22284)

NAT32® is a versatile IP Router implemented as a WIN32 application.


Vulnerability Type:
===================
Remote Command Execution (CSRF)


CVE Reference:
==============
CVE-2018-6941


Security Issue:
================
CSRF issue exists in the HTTPD component of NAT32 v2.2 Build 22284 devices that can be exploited for Remote Co

Remote attackers can potentially execute arbitrary System Commands due to a Cross Site Request Forgery, if an
or visits an attacker controlled webpage as NAT32 performs no check for blind requests.

Its also worth mentioning is NAT32 implements BASIC authentication which pass BASE64 Encoded credentials which


Exploit/POC:
```

```
Network Access:
===============
Remote



Severity:
=========
High



Disclosure Timeline:
=============================
Vendor Notification: February 9, 2018
Vendor acknowledgement: February 9, 2018
Vendor "I've decided to remove the HTTPD code from Build 22284 of NAT32" : February 12, 2018
www.nat32.com website reads "NAT32 Version 2.2 Build 22284 is temporarily unavailable." : February 13, 2018
February 14, 2018 : Public Disclosure



[+] Disclaimer
The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness
Permission is hereby granted for the redistribution of this advisory, provided that it is not altered except b
that due credit is given. Permission is explicitly given for insertion in vulnerability databases and similar,
is given to the author. The author is not responsible for any misuse of the information contained herein and a
for any damage caused by the use or misuse of this information. The author prohibits any malicious use of secu
or exploits by the author or elsewhere. All content (c).
```

**Source:** www.exploit-db.com

# ← Exploit Collector


KitPloit - PenTe...

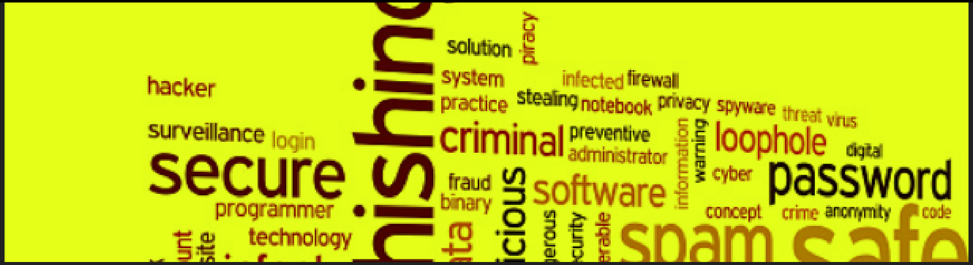
Like Page

Follow @KitPloit  101K followers

KitPloit

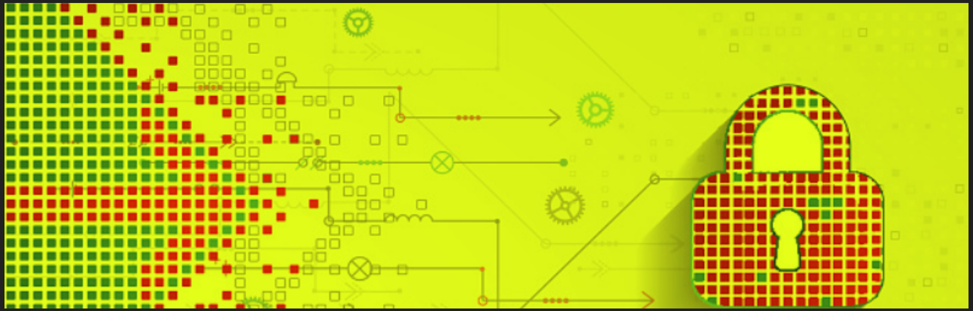
google.com/+KitploitWeb

G+ Follow



## Linux/x86 Read /etc/passwd Shellcode

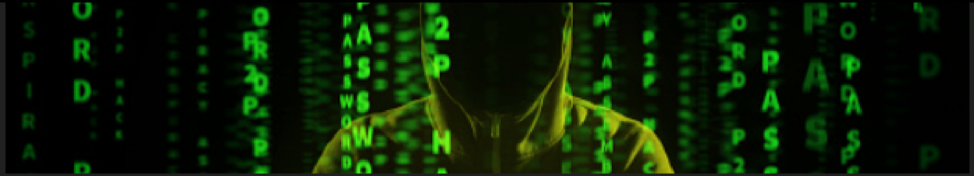
*62 bytes small Linux/x86 read /etc/passwd shellcode.*



## Microsoft Internet Explorer VBScript Engine CVE-2018-8174 Arbitrary Code Execution Vulnerability

*Microsoft Internet Explorer is prone to an unspecified arbitrary code-execution vulnerability.*

*Attackers can exploit this vulnerability to execute arbitrary code in the* …



WhatsApp 2.18.31 iOS Memory Corruption

*WhatsApp version 2.18.31 on iOS suffers from a remote memory corruption vulnerability.*

Archive