

Security at the Switch



Why should I patch my networking equipment?

Who am I?

- Threat Researcher at Aruba Threat Labs, the internal Red Team for Aruba Networks
- Proud member of ISSA and SecDSM (<https://secdsm.org>)
- Local to Des Moines!
- Network/IoT device hacking enthusiast extraordinaire

What is this talk about?

This talk is about the potential security issues that can arise from a malicious actor exploiting vulnerabilities in network hardware.

- Switches
- Routers
- Enterprise equipment
- Small Office / Home Office equipment.

ExploitDB

~50,000 Exploits listed in total.

~1,600 are hardware: <https://www.exploit-db.com/?platform=hardware>

We'll use this dataset as our primary resource

We will focus on the Web administration interface for this talk, but briefly talk about other avenues of attack.

What kind of problems will I find?

Standard Web App stuff:

- Cross Site Scripting
- CSRF
- Broken Authentication
- Information Leaks

Cross Site Scripting (XSS)

Allows an attacker to issue state changing operations on behalf of the administrator by executing arbitrary JavaScript in the admin's browser

Can be used to do things like

- Change administrator password
- Re-configure VLANs
- Modify Upstream DNS Server Address

Mitigated by sanitizing all input

Cross Site Request Forgery (CSRF)

Allows an attacker to issue state changing operations on behalf of the administrator by abusing the trust a web application has for a browser.

Can be used to do things similar to Cross-site Scripting

Mitigated by adding Anti-CSRF Token to HTML output of application, and checking those tokens on the server.

Broken Authentication

Allows an attacker to issue bypass, reset, or change from an unauthenticated position authentication credentials for administration of a device.

Information Leaks

SNMP is a vastly abused service for gleaning all sorts of useful information for an attacker.

- All DHCP Leases and their address / hostnames
- Administrative Credentials
- Current state tables

Ok but what about the fun stuff

Things you will find in networking gear that you almost never see in standard web apps:

- Command Injection
- Buffer Overflows

Command Injection

Calls to ``system`` which include unsanitized user input.

- Almost always leads to system compromise

Why does this almost always lead to system compromise?

Everything runs as root

I've only seen a single device that had non-privileged accounts that the web service was running as.

Buffer Overflow

Most Networking Web Interfaces are written in C from scratch.

Basic binary hardening protections are not enabled in the majority of SoHo equipment.

ASLR/DEP could make building exploits way more difficult

Good hackers read the classics

Reviewing others' exploits helps build a base of knowledge for finding your own security issues!

Some Examples

- <https://www.exploit-db.com/exploits/2059>
- <https://www.exploit-db.com/exploits/39823>
- <https://blog.senr.io/devilsivy.html>
- <https://github.com/threat9/routersploit>
- https://github.com/threat9/routersploit/blob/master/routersploit/modules/exploits/routers/belkin/n750_rce.py
- https://github.com/threat9/routersploit/blob/master/routersploit/modules/exploits/routers/netgear/multi_rce.py

Let's look at these examples to see what is going on!

More Examples

- https://github.com/beefproject/beef/blob/9f1e8f5e8d34b1ee0bad84636da4bd6f6073e403/modules/exploits/switch/dlink_dgs_1100_fdb_whitelist/command.js
- https://github.com/beefproject/beef/blob/9f1e8f5e8d34b1ee0bad84636da4bd6f6073e403/modules/exploits/switch/dlink_dgs_1100_device_reset/command.js
- https://github.com/beefproject/beef/blob/9f1e8f5e8d34b1ee0bad84636da4bd6f6073e403/modules/exploits/switch/dlink_dgs_1100_port_mirroring/command.js

Beef Framework: <https://github.com/beefproject/beef>

Impact

Why should I care?

In recent history, the biggest malicious use for pwnd networking equipment is a botnet.

Mirai and all its clones are the best example.

Scenario I

- 1) An attacker seizes control of your home router.
- 2) The attacker changes your upstream DNS server to an attacker controlled DNS Server
- 3) You try to access your bank
- 4) Attacker sends a bad IP back and your browser loads attacker controlled Bank
- 5) You log in
- 6) Your money gets deleted

Scenario II

- 1) You have set up network monitoring to catch large data dumps to external destinations
- 2) An attacker pwns your core switch
- 3) An attacker turns your core switch into a packet filter
- 4) You fail to see all the data leaving your network
- 5) Brian Krebs alerts you to your data breach

Fallout

An attacker that is able to control your networking infrastructure can severely disrupt business operations for your organization.

Attackers read vendor advisories and use them to create exploits

Just because the vendor advisory doesn't have all the details does not mean a determined attacker cannot figure it out.

Questions?

Contact:

@nstarke (Twitter)

@nstarke (SecDSM Slack)