DHCXSSP

Hey

- CompSci student at KIT Karlsruhe
- shackspace
- @momorientes
- m@hackathon.de


Ethernet
Power
DMZ
WLAN
1
2
3
4
Internet
Broadband Router
With 4-Port Switch
ENTERPRISE!!!11

Webinterface vulnerabilities

- XSS in search fields
- Username SQL Injections
- XSRF
- ...

might be interesting but has been done >9000 times and mostly requires access to the management network

Other attack vectors?

hostname	IP	mac	comment
foo	192.168.1.23	DE:AD:BE:EF	boss
bar	192.168.1.42	B0:0B:51:01	Secretary
blaaah	192.168.1.222	12:34:56:78	<script>alert(1)</script>
...	...	...	...

meh.

hostname	IP	mac	comment
foo	192.168.1.23	DE:AD:BE:EF	boss
bar	192.168.1.42	B0:0B:51:01	Secretary
blaaah	192.168.1.222	12:34:56:78	accounting
...	...	...	...

DHCP Hostname

- RFC 2132 – 3.14
- “... minimum length is 1”
- max. length is not specified, but most vendors stick to 32 – 64 chars
- alphanumerical with special chars \o/

sudo dhcpcd -h “\"><script>alert(1)</script>” wlan0

things to make your life easier

- Those things have weird caching, for testing switch your mac address on every try
- The dot may be considered for domain and everything thereafter might be ignored
- If you need IP addresses for your xss try dword

outcome

- ~15 vendors affected
- Most of them patched it

But who does updates anyways?

More fun with DHCXSSP

- DHCP Next Server and other DHCP settings might not be supported by the devices and can raise malicious log messages (cheers FX)
- Works in theory but didn't find any vulnerable webinterfaces (yet)

And now what?

- I can't get my hands on any crappy webinterface ever deployed, but WE can
- If you find something contact the vendor and disclose responsibly
- Let me know if you find something and get me a tschunk
- We already tested the GPN network, no fun to be had here :(