nieldk Update Admin bypass History

1 contributor

53 lines (40 sloc) | 2.02 KB

```
NBG2105 Mini Travel Router
Local admin bypass

CVE-2021-3297

The NBG2105 is a Wireless Mini Travel Router by ZyXel, information and downloads can be found here https://www.zyxel.com/support/SupportLandingSR.shtml?c=gb&l=en&kbid=M-01490&md=NE

I discovered a vulnerability, which allows anyone to access to routers administrative configuration pages.

The Javascript located at the router on http://router-IP/js/util_gw.js exposes the function checkCookie(), which reveals the cookie "login".
Initially the value of this cookie is "0", but the cookie is set to "1" after a successful login.

This can be abused to gain access to the routers administration page, without login credentials, by setting the document cookie "login" to "1".

The part of the javacode exposing this check is shown below where it checks this value by the statement "if(login != 1)":
Any other cookie content than "1" will return to the router login page.

function checkCookie()
{
        var login=0;
        if(document.cookie.length > 0)
        {
                var first = document.cookie.indexOf("login=");
                var second = document.cookie.indexOf(";", first);
                if(first != -1)
                {
                        if(second == -1)
                                login = document.cookie.substring(first+6);
                        else
                                login = document.cookie.substring(first+6, second);
                }
        }

        if(login != 1)
                MM_goToURL('parent', 'login.htm');
}


Furthermore, it is possible to bypass the login, by calling the static web page,
located at  http://router-IP/login_ok.htm which will set the cookie "login" to "1" and thus bypass the login credentials check.

This can be observed in the below code from util_gw.js

function setCookie() //login_ok.htm use
{
        document.cookie="login=1";
        MM_goToURL('parent', 'home.htm');
}

Timeline
24. Jan 2021 reported to Zyxel
25. Jan 2021 Zyxel confirm recieved report
27. Jan 2021 Zyxel respond with wont-fix (EOL)
```