MWR LABS

Security Advisory

Symantec Endpoint Protection Manager – Directory Traversal

2016-07-03

Software	Symantec Endpoint Protection Manager
Affected Versions	12.1.6 MP1
CVE Reference	CVE-2016-5307
Author	Che Lin Law
Severity	Medium
Vendor	Symantec
Vendor Response	Patch released as part of 12.1-RU6-MP5

Description

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, and servers in corporate networks against malware, risks, and vulnerabilities. Symantec Endpoint Protection Manager is the management server component that manages the client computers with Symantec Endpoint Protection enabled.

Symantec Endpoint Protection Manager contained a directory traversal vulnerability that allowed unauthenticated users access to arbitrary files on the server.

Impact

This vulnerability would allow unauthenticated threat agents unauthorised access to resources on the server. These resources may contain sensitive information such as configuration files, log files and/or source codes.

Interim Workaround

Ensure that no sensitive files are stored within the web root directory.

Solution

Update to Symantec Endpoint Protection Manager 12.1-RU6-MP5.

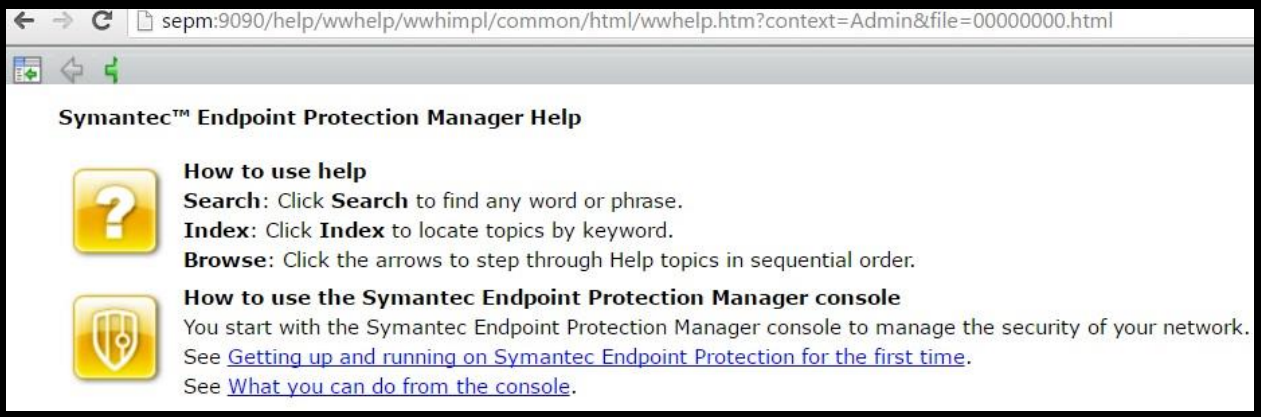
Technical details

Symantec Endpoint Protection Manager contained a help interface that referenced files on the server using the "file" parameter.

An example of this is as follows:

```
http://sepm:9090/help/wwhelp/wwhimpl/common/html/wwhelp.htm?context=Admin&file=00000000.html
```

A screenshot of the file, "00000000.html ", being loaded is as follows:



A proof of concept URL was created to demonstrate how the "file" parameter could be exploited to perform directory traversal:

```
http://sepm:9090/help/wwhelp/wwhimpl/common/html/wwhelp.htm?context=Admin&file=../success.jpg
```

This screenshot demonstrates the file, "success.jpg", being loaded from the web root directory:

Further Information

https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160628_01

Detailed Timeline

Date	Summary
02 Mar 2016	Issue reported to Symantec
04 Mar 2016	Symantec confirms recipient and will review issue
01 Apr 2016	MWR requests update
04 Apr 2016	Symantec confirms issue and a patch will be issued in the next release
25 May 2016	Symantec updates MWR that issue will be fixed as part of version 12.1.6 MP5
28 Jun 2016	Patch released as part of 12.1-RU6-MP5