National Computer Board
Computer Emergency Response Team of Mauritius
(CERT-MU)

Threat Alert

Symantec Endpoint Protection Multiple Issues

Issued on: August 03, 2015

Severity Rating: High

Systems Affected:

- Symantec Endpoint Protection Manager Version 12.1
- Symantec Endpoint Protection Clients Version 12.1

Overview:

Multiple vulnerabilities have been identified in Symantec and can be exploited by remote attackers to conduct SQL injection, authentication bypass, read or write files and gain elevated privileges on the vulnerable system. Symantec has released updates to address these vulnerabilities.

Description:

Multiple vulnerabilities have been identified in Symantec and can be exploited by remote attackers to conduct SQL injection, authentication bypass, read or write files and gain elevated privileges on the vulnerable system. The vulnerabilities reside in the management console for Symantec Endpoint Protection Manager (SEPM). The vulnerabilities reported are as follows:

1. The management console for SEPM is vulnerable to a manipulation of the password reset functionality and this could be exploited by remote attackers to generate the creation of a new administrative session and assigned to the requestor. The new session can be used to bypass proper authentication to access the server.
2. A vulnerability exists due to improper file name validation in a console session and this could be exploited by remote attackers to allow an authorized SEPM user to write arbitrary files in the context of the corresponding user.
3. An arbitrary file read vulnerability occurs due to improper validation in one of the action handlers. This could allow an authenticated user to read arbitrary files as they may not have authorized access to. Successful exploitation of the vulnerability can allow an authorized, but less privileged user to manipulate SEPM services to launch arbitrary code with administrator privileges.
4. A vulnerability exists because SEPM does not properly validate or sanitise SQL input and can be exploited by remote attackers to run an unauthorized arbitrary SQL query

against the backend database. Successful exploitation of the vulnerability can allow access to or manipulation of data resulting in potential unauthorized access to restricted server-side data and possible ability to leverage additional console management functionality.

5. There is a path traversal issue which occurs during the importing of a client installation package to SEPM because the package is not sufficiently validated or sanitized during the process. This could allow a remote attacker to submit a specifically configured package containing a relative path of their creation in an attempt to access files and/or directories external to the authorized install folder.
6. The SEP clients are susceptible to a potential binary attack/dll preloading issue resulting from not properly restrict the loading of external libraries. This vulnerability can allow a user with access to a system to insert a specifically-crafted library into a client install package. Successful exploitation could allow unauthorized arbitrary code to be executed with system privileges.

CVE Information

CVE-2015-1486

CVE-2015-1487

CVE-2015-1488

CVE-2015-1489

CVE-2015-1490

CVE-2015-1491

CVE-2015-1492

Workarounds

Users are advised to apply updates.
More information about the update is available on:
http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20150730_00

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert-mu.gov.mu

Incident: incident@cert-mu.gov.mu

Website: http://www.cert-mu.org.mu