CERT-MU AD-2016-01

# Multiple Vulnerabilities in Symantec Endpoint Protection

**Original Issue Date:** 30 June 2016

**Severity Rating:** High

**Overview:**

Multiple vulnerabilities have been identified in Symantec Endpoint Protection (SEP). These vulnerabilities could be exploited by remote attackers to gain elevated privilege or access to unauthorised files on the management console.

Moreover, attackers can bypass security restrictions allowing some level of access to file download or upload on a client system by forcing a race condition in the device control of a SEP client.

**Description:**

Multiple vulnerabilities have been identified in Symantec Endpoint Protection (SEP). These vulnerabilities can be exploited by a lower-privileged user or by an unauthorised user to elevate privilege or gain access to unauthorized information on the management server. Exploitation attempts of these vulnerabilities requires access to the SEP Management console.

The vulnerabilities can be exploited by remote attackers by:

- Conducting cross-site request forgery and server-side request forgery attacks, where an attacker can view files on the target system. A local user can bypass security restrictions. A remote user can redirect the target user's browser to an arbitrary site. A remote authenticated user can obtain passwords on the target system. A remote authenticated user can bypass security restrictions. A remote user can conduct cross-site scripting attacks. These vulnerabilities are due to poor validation and sanitation of user input and server output.

- Creating a specially crafted HTML page or URL that, when loaded by the target authenticated user, will take actions on the target management interface impersonating the target user.
- Using brute-force password attack to bypass the lock threshold limits to recover valid management console passwords.
- Manipulating the GET object requests to gather information on other valid system administrator accounts. This can be done using brute force attack.
- Creating a URL that, when loaded by the target user, will redirect the target user's browser to an arbitrary site.
- Exploiting an existing DOM link manipulation weakness (a type of XSS) in existing management scripts to attempt attacks against managed client systems.
- Not effectively enabling HTTP Strict Transport Security on port 8445, the SEPM listening port, could lead to information leakage or redirection-type attacks.
- There is a limited access directory traversal in the management console which could allow a less-privileged user to access files/directories on the web root.

**Impact of the attack(s)**

A remote attacker can impersonate an authenticated user, view files, cause the target user browser to be redirected to an arbitrary web site, bypass security controls, take actions on the target system acting as the target authenticated user, obtain passwords on the target system, access the target user's cookies (including authentication cookies), access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user and cause the target server to connect to arbitrary ports on arbitrary hosts.

**Affected System:**

Symantec Endpoint Protection Manager and client, version 12.1

**CVE Information:**

CVE-2015-8801

CVE-2016-3647

CVE-2016-3648

CVE-2016-3649

CVE-2016-3650

CVE-2016-3651

CVE-2016-3652

CVE-2016-3653

CVE-2016-5304

CVE-2016-5305

CVE-2016-5306

CVE-2016-5307

**Solution**

Users are advised to apply updates.

More information about the updates is available on:

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

**Best Practices**

As part of normal best practices, the following is strongly recommended:

- Restrict access to administrative or management systems to authorized privileged users.
- Restrict remote access, if required, to trusted/authorized systems only.
- Run under the principle of least privilege where possible to limit the impact of potential exploit.
- Keep all operating systems and applications current with vendor patches.
- Follow a multi-layered approach to security. At a minimum, run both firewall and anti-malware applications to provide multiple points of detection and protection to both inbound and outbound threats.
- Deploy network- and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in the detection of attacks or malicious activity related to the exploitation of latent vulnerabilities.

**References:**

**Security Tracker**

http://securitytracker.com/id/1036196

**Symantec**

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

**Disclaimer**

The information provided herein is on "as is" basis, without warranty of any kind. Please note that the members who do not want to receive the security alert, can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

**Hotline No:** (+230) 800 2378
**Fax No:** (+230) 208 0119
**Gen. Info**. : contact@cert.ncb.mu
**Incident:** incident@cert.ncb.mu
**Website:** http://cert-mu.org.mu