# Microsoft Management Console (MMC) Vulnerabilities - Check Point Research

By deugenio

Published: 2019-06-11 · Archived: 2026-04-05 15:10:43 UTC

*Research by: Eran Vaknin and Alon Boxiner*

The goal of Microsoft Management Console (MMC) is to provide a programming platform for creating and hosting applications that manage Microsoft Windows-based environment, and to provide a simple, consistent and integrated management user interface and administration model.

Recently, Check Point Research discovered several vulnerabilities in the console that would allow an attacker to deliver a malicious payload.

Microsoft has granted CVE-2019-0948 to this vulnerability and patched it in their June 11th Patch Tuesday release.

**Vulnerability Description:**

**1) Multiple XSS vulnerabilities due to misconfigured WebView.**

MMC has an integrated Snap-In component which in turn contains several mechanisms such as ActiveX Control, Link to Web Address, etc.

1. As an attacker chooses the Link to Web Address snap-in, he can insert a url to his server which contains an html page with a malicious payload.
   As the victim opens the malicious .msc file, a web-view is opened (within the MMC window) and the malicious payload is executed.
   We have successfully managed to insert malicious URL link that contains malicious payloads such as redirection to SMB server that will capture the user NTLM hash.
   Moreover, it is also possible to execute VBS script on the victims' host via the mentioned web-view.
2. An attacker chooses the ActiveX Control snap-in (all ActiveX controls are vulnerable) and saves it to file (.msc file). In the .msc file, under the StringsTables section, the attacker changes the third string value to malicious url under his control, containing an html page with a malicious payload. As mentions in sections a (above) – we have successfully managed to insert malicious URL link that contains malicious payloads such as redirection to SMB server that will capture the user NTLM hash.
   Moreover, it is also possible to execute VBS script on the victims' host via the mentioned web-view.
   As the victim opens the malicious .msc file, a web-view is opened (within the MMC window) and the malicious payload is executed.

**2) XXE Vulnerability due to misconfigured XML parser.**

A victim opens the MMC and chooses the event viewer snap-in and clicks on Action and then on Import Custom View. As soon as a malicious XML file is chosen (containing an XXE payload) any file from the victims host is sent to the attacker.
This is possible due to a misconfigured XML parser defined within the MMC custom view functionality.

**Proof of Concept**

**1) Link to Web Address snap-in Cross-Site Scripting (XSS):**

The attacker adds a new snap-in:

The victim chooses a Link to Web Address snap in:

The attacker then types the path to his server containing the malicious payload:

The attacker saves the .msc file and sends it to the victim:

The malicious .msc file contains the path to the attacker’s server:

**As the victim** opens the malicious .msc file VBS code is executed:

**2) ActiveX Control snap-ins: (Adobe Acrobat DC Browser example):**

The attacker adds a new snap-in:

The attacker chooses an ActiveX Control snap-in:

The ActiveX Control mechanism is then chosen (Adobe Acrobat DC Browser as an example):

The attacker saves the .msc file and sends it to the victim:

The malicious .msc file containing the path to the attacker’s server:

**As the victim** opens the malicious .msc file VBS code is executed:

**3) XXE Vulnerability Due to Misconfigured XML Parser:**

Add a snap-in:

The attacker chooses the event viewer snap-in:

The victim selects ‘Action’ and then clicks on the ‘Import Custom View’ option:

The victim selects the malicious XML sent by the attacker

The malicious XML containing the XXE payload will read the c:\windows\win.ini file content and send it to the remote server via HTTP/GET request:

Which in turn will call to xml.dtd:

The desired file content is sent from the client console application to a remote server:

---

Source: https://research.checkpoint.com/2019/microsoft-management-console-mmc-vulnerabilities/