



Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Critical RCE Vulnerability Found in Symantec Endpoint Management Platform

Vulnerability Note: VN-2025-11

Date of Issue: 15 July 2025

Severity Rating: High

Systems Affected:

- Broadcom Symantec Endpoint Management Suite (Altiris) versions 8.6.x, 8.7.x, 8.8

Description

A critical remote code execution (RCE) vulnerability has been identified in Broadcom's Symantec Endpoint Management Suite formerly known as Altiris. This vulnerability can be exploited by remote attackers to cause execution of arbitrary code on vulnerable systems. The vulnerability is caused due to an exposed legacy .NET Remoting endpoint in the Symantec Altiris Inventory Rule Management (IRM) component accessible at:
`tcp://<host>:4011/IRM/HostedService`.

When this endpoint is reachable over the network, it enables attackers to exploit insecure deserialization of .NET objects, leading to complete system compromise without requiring authentication.

CVE Information

[CVE-2025-5333](#)

Workaround

- The primary mitigation involves ensuring port 4011 is closed on the Notification Server firewall, as official documentation does not require this port to be opened.
- Additionally, administrators can configure the `IRM_HostedServiceUrl` setting to remain empty, restricting .NET Remoting access to localhost only.
- Broadcom has indicated that future product releases will include enhanced security measures to limit and secure the use of .NET Remoting for the IRM/HostedService component, preventing remote access to this potentially dangerous endpoint.

- Organisations using affected versions should immediately review their firewall configurations and implement the recommended mitigations to prevent exploitation of this critical vulnerability.

Postal address

Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,