مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical RCE Vulnerability in Broadcom Symantec Endpoint Management

Tracking #:432317489

Date:16-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical remote code execution (RCE) vulnerability, CVE-2025-5333, has been discovered in Broadcom’s Symantec Endpoint Management Suite, previously known as Altiris.

TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability, CVE-2025-5333, has been discovered in Broadcom’s Symantec Endpoint Management Suite, previously known as Altiris. This flaw stems from an exposed legacy .NET Remoting endpoint (tcp://<host>:4011/IRM/HostedService) in the Inventory Rule Management (IRM) component, which is vulnerable to insecure object deserialization.
Attackers can leverage this vulnerability to execute arbitrary code **without authentication**, resulting in complete system compromise. The vulnerability has a **CVSS v4.0 base score of 9.5 (Critical)**. Immediate action is required to mitigate risk in affected enterprise environments.

Vulnerability Details:

- CVE ID: CVE-2025-5333
- Severity: Critical (CVSS v4.0 Score: 9.5)
- Affected Product: Broadcom Symantec Endpoint Management Suite (Altiris)
- Affected Versions: 8.6.x, 8.7.x, 8.8
- Attack Vector: Remote (Unauthenticated)
- Impact: Remote Code Execution (RCE), System Compromise
- Exploit Status: Exploitable in the wild (confirmed in lab)

Vendor Response

Broadcom's Product Security Incident Response Team (PSIRT) has acknowledged the vulnerability and provided the following guidance:

- Port 4011 is not required to be open based on official documentation.
- Configuration options should be updated to restrict access to localhost.
- Future versions will deprecate or secure use of .NET Remoting for IRM/HostedService

RECOMMENDATIONS:

Restrict Network Access to Port 4011

- Block **TCP port 4011** on all firewall layers (host, network perimeter) for servers running Altiris Notification Server.
- Validate that port 4011 is not accessible from untrusted networks or internet-facing interfaces.

Patch When Available

- Stay informed on official patches or updates from Broadcom PSIRT.
- Apply security updates to mitigate this issue once released

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-5333