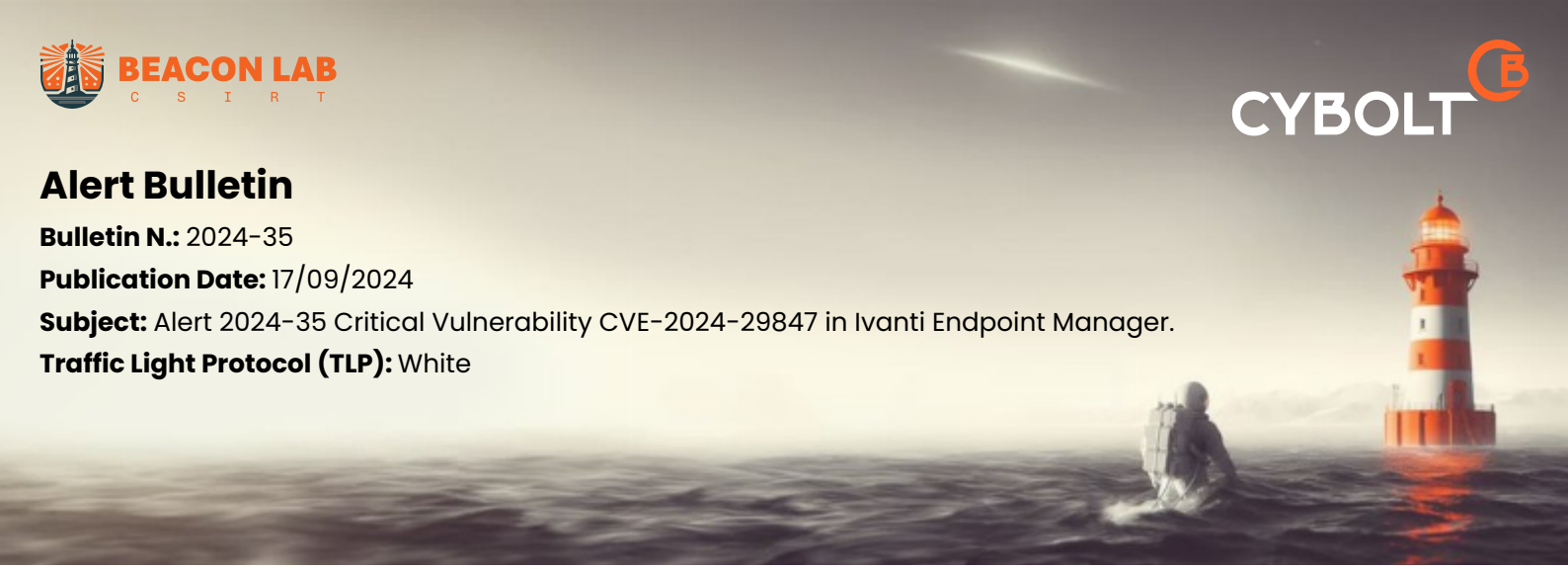

Alert Bulletin

Bulletin N.: 2024-35
Publication Date: 17/09/2024
Subject: Alert 2024-35 Critical Vulnerability CVE-2024-29847 in Ivanti Endpoint Manager.
Traffic Light Protocol (TLP): White

Affected Product(s):

- Ivanti Endpoint Manager (EPM) 2024 and 2022 SU5 and earlier versions

Description:

Ivanti Endpoint Manager (EPM) is an enterprise endpoint management solution that enables centralized device management within an organization.

Ivanti has released updates for Ivanti Endpoint Manager 2024 and 2022 SU6 that address medium and high-severity vulnerabilities. Successful exploitation of these vulnerabilities could allow unauthorized access to the central EPM server.

One of the critical vulnerabilities is CVE-2024-29847. This vulnerability arises from the deserialization of untrusted data in the Ivanti EPM agent portal, affecting versions prior to 2022 SU6 and the September 2024 update. This flaw allows an unauthenticated remote attacker to execute code remotely, with a CVSS score of 10.0.

Within the AgentPortal.exe executable, the LANDesk.AgentPortal.AgentPortal.OnStart method is invoked every time the “Agent Portal” service starts. This service runs by default, and its exploitation can enable unauthenticated remote code execution.

The vulnerability lies in the use of .NET Remoting, a technology strictly prohibited by Microsoft due to its risks but still found in many critical infrastructures. By leveraging .NET Remoting and various techniques, an attacker can achieve remote code execution, potentially allowing the attacker to run arbitrary code on the server and manipulate files and commands.