Proactive Notification: Critical Alert

12 July 2017

Dear CA Customer:

The purpose of this Critical Alert is to inform customers of a vulnerability with the Unified Management Portal (UMP) component of Unified Infrastructure Management (UIM). Please read the information provided and follow the instructions below.

PRODUCT(S) AFFECTED:
Unified Infrastructure Manager (UMP) Releases: 7.5 - 8.5.1

PROBLEM DESCRIPTION:
A critical vulnerability has been discovered in the Liferay framework within the Unified Management Portal. This vulnerability could allow a remote attacker to gain full control of the server running UMP.

SYMPTOMS:
HTTP or HTTPS POST requests sent to the following endpoints result in a 200 OK response rather than a 403 Forbidden, indicating that the Liferay security filter may be bypassed:

- /api/liferay;
- /api/secure/liferay;
- /api/spring;
- /api/secure/spring;

IMPACT:
By exploiting this vulnerability, an attacker can gain remote access to the UMP server and execute commands as root/administrator on the compromised system.

Proactive Notification: Critical Alert

TEMPORARY REMEDIATION:

1. Download and install ump-hf1 package via Admin Console or Infrastructure Manager on all systems running UMP 7.5-8.5.1.

Note: If UMP is reinstalled from the default installation package, the ump-hf1 security policy changes will not persist and will need to be reinstalled as described above.

VALIDATION:
HTTP or HTTPS POST requests sent to the listed endpoints through a tool such as Postman or a web browser should result in a 404 response.

- /api/liferay
- /api/secure/liferay
- /api/spring
- /api/secure/spring

PROBLEM RESOLUTION:
This patch is a mitigation to limit access to the vulnerable endpoints. Further attacks to these endpoints are possible if these attacks originate from trusted IP addresses. CA is working with Liferay to provide a final resolution to this vulnerability for all Liferay content. Further updates will follow.

If you have any questions about this Critical Alert, please contact CA Support.

Thank you,
CA Support Team