Advisory Alert

Alert Number: AAA20230314 **Date:** March 14, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Cross-Site Scripting Vulnerability

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Cross-Site Scripting Vulnerability (CVE-2023-28083)
Description	HPE has released a security update addressing Cross-Site Scripting vulnerability that can be remotely exploited in HPE Integrated Lights-Out 6 (iLO 6), Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 4 (iLO 4). HPE recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	HPE Integrated Lights-Out 6 (iLO 6) before v1.20 for: ProLiant Gen11 servers. HPE Integrated Lights-Out 5 (iLO 5) before v2.78 for: ProLiant Gen10 and Gen10 Plus servers. Synergy compute modules. Apollo chassis, servers, and systems. Converged systems. StoreEasy Storage. HPE Integrated Lights-Out 4 (iLO 4) before v2.82 for: ProLiant Gen8 and Gen9 servers. Synergy compute modules. Apollo chassis and servers Converged systems. StoreEasy Storage. 3PAR StoreServ Controllers.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04456en_us

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.