Advisory Alert

Alert Number: AAA20210712 **Date:** July 12, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Kesaya	**Critical**	Multiple vulnerabilities
HPE	**High**	Multiple vulnerabilities

Description

Affected Product	Kesaya
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-30116,CVE-2021-30119,CVE-2021-30120,CVE-2021-30117,CVE-2021-30118,CVE-2021-30121,CVE-2021-30201)
Description	Kesaya has released security updates addressing multiple vulnerabilities that exists in their products including Credentials leak and business logic flaw, Cross-site scripting vulnerability, Two-factor authentication bypass, SQL injection vulnerability,Remote code execution vulnerability,Local file inclusion vulnerability,XML external entity vulnerability. Kesaya recommends to apply necessary security fixes to avoid issues.
Affected Products	prior to update Kaseya VSA 9.5.7a
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://helpdesk.kaseya.com/hc/en-gb/articles/4403785889041

Affected Product	HPE
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-14386,CVE-2021-3156,CVE-2021-29150,CVE-2021-29151,CVE-2021-29152,CVE-2021-34609,CVE-2021-34610,CVE-2021-34611,CVE-2021-34612,CVE-2021-34613,CVE-2021-34614,CVE-2021-34615,CVE-2021-34616)
Description	HPE has released security updates addressing multiple vulnerabilities that exists in their clear policy manager product including Privilege escalation, Arbitrary Command Execution, Authentication Bypass, Denial of Service, SQL Injection and Insecure Deserialization. HPE highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	ClearPass 6.9.x prior to 6.9.6 ClearPass 6.8.x prior to 6.8.9 ClearPass 6.7.x all versions ClearPass 6.6.x all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04181en_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.