TLP: WHITE

Advisory Alert

Alert Number : AAA20201027 **Date :** October 27, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HP	High	Remote authentication bypass
IBM	High	Denial of service

Description

Affected Product	HP
Severity	High
Affected Vulnerability	Remote authentication bypass (CVE-2020-7197)
Description	HP has released security updates addressing vulnerability that exists in HPE StoreServ Management Console. This flaw allows a remote attacker to bypass authentication process. This flaw exists due to an error in when processing authentication requests in HPE 3PAR StoreServ Management and Core Software Media. A remote attacker can bypass authentication process and gain unauthorized access to the application. It is highly recommended this should be acted upon as soon as possible.
Affected Products	HPE 3PAR StoreServ Management and Core Software Media prior to 3.7.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-hpesbst04045en_us

Affected Product	IBM
Severity	High
Affected Vulnerability	Denial of service (CVE-2020-11868, CVE-2020-13817, CVE-2020-15025)
Description	IBM has released security patch updates addressing denial of service vulnerabilities that exists in NTPv4 with their products. It is highly recommended to apply necessary fixes to the IBM products to avoid issues. CVE-2020-15025 – This flaw allows remote attackers to cause a denial of service (memory consumption) by sending specially crafted packets, because memory is not freed in situations where a CMAC key is used and associated with a CMAC algorithm in the ntp.keys file. CVE-2020-13817 – This flaw allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources and there must be an off-path attacker who can query time from the victim's ntpd instance. CVE-2020-11868 – This flaw allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address.
Affected Products	AIX 7.1, 7.2, VIOS 3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6353453

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.