Advisory Alert

Alert Number : AAA20200925 **Date :** September 25, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Fortinet	**High**	Multiple Vulnerabilities
Citrix	**High**	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3503, CVE-2020-3526, CVE-2020-3552, CVE-2020-3559, CVE-2020-3560, CVE-2020-3409, CVE-2020-3512, CVE-2020-3400, CVE-2020-3516, CVE-2020-3393, CVE-2020-3396, CVE-2020-3511, CVE-2020-3477, CVE-2020-3479, CVE-2020-3408, CVE-2020-3510, CVE-2020-3359, CVE-2020-3492, CVE-2020-3527, CVE-2020-3417, CVE-2020-3423, CVE-2020-3476, CVE-2020-3403, CVE-2020-3404, CVE-2020-3480)
Description	Cisco has released patches/updates addressing multiple vulnerabilities that exists in various products including Cisco IOS and IOS XE software. It is highly recommended to apply necessary fixes provided in official Cisco website at earliest to avoid these vulnerabilities.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x

Affected Product	HPE
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-11896, CVE-2020-11898, CVE-2020-11900, CVE-2020-11906, CVE-2020-11907, CVE-2020-11911, CVE-2020-11912, CVE-2020-11914)
Description	HPE released patch upgrades addressing remote code execution, denial of service, information disclosure vulnerabilities that exists in iLO4 for Superdome X Servers. And it is recommended to apply necessary fixes provided by HPE as soon as possible to mitigate these vulnerabilities.
Affected Products	HPE Integrity Superdome X with BL920s Gen8 Server Blade - Prior to bundle 8.8.38 HPE Integrity Superdome X with BL920s Blades - Prior to bundle 8.8.38 HPE Integrity Superdome X with BL920s Gen9 Server Blade - Prior to bundle 8.8.38
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04038en_us

Affected Product	**Fortinet**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-12820, CVE-2020-12819, CVE-2020-12816)
Description	Fortinet requests from their product consumers to perform firmware upgrades at earliest on multiple devices that are running below firmware versions in order to avoid vulnerability exposures. **CVE-2020-12820:** Stack-based buffer overflow in SSL VPN daemon may allow a remote attacker authenticated to the SSL VPN to crash the FortiClient Network access controller daemon and execute arbitrary codes through requesting a large FortiClient file name. **CVE-2020-12819:** FortiOS is potentially vulnerable to a Heap buffer overflow allowing a remote attacker with valid SSL VPN credentials to crash the SSL VPN daemon by sending large LCP packets. **CVE-2020-12816:** A remote authenticated attacker can perform a stored XSS attack via User ID of admin users by exploiting the improper neutralization of inputs in FortiNAC.
Affected Products	FortiNAC version 8.7.2 and below FortiOS versions 5.6.12, 6.0.10, 6.2.4, 6.4.1 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://fortiguard.com/psirt/FG-IR-20-083 https://www.fortiguard.com/psirt/FG-IR-20-082 https://www.fortiguard.com/psirt/FG-IR-20-002

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-25603, CVE-2020-25595, CVE-2020-25597, CVE-2020-25604, CVE-2020-25596, CVE-2020-25601, CVE-2020-25600, CVE-2020-25599, CVE-2020-25602) (CVE-2020-25598,
Description	Citrix and Xen project has released security fixes addressing multiple vulnerabilities that exists in their products. Citrix recommends that affected users to install these hotfixes at earliest after downloading from the official Citrix and Xen project website. And technical support is available for Citrix commercial products.
Affected Products	Citrix Hypervisor, XenServer 7.1,7.0 Multiple Xen versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	http://xenbits.xen.org/xsa https://support.citrix.com/article/CTX282314