TLP: WHITE

Advisory Alert

Alert Number : AAA20201015 **Date:** October 15, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SONICWALL	High	Multiple Vulnerabilities
RedHat	Medium	Use-after-free
Python	Medium	Multiple Vulnerabilities

Description

Affected Product	SONICWALL
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-5135)
Description	Vulnerability was found in SONICWALL which allows a remote attacker to cause denial of service (DOS) attack and to execute arbitrary codes by sending malicious requests to the firewall. There are no workarounds and SONCWALL has released patch updates addressing this vulnerability. It is highly recommended to apply these patches at earliest to avoid such issues.
Affected Products	SonicOS 6.5.4.7-79n and earlier SonicOS 6.5.1.11-4n and earlier SonicOS 6.0.5.3-93o and earlier SonicOSv 6.5.4.4-44v-21-794 and earlier SonicOS 7.0.0.0-1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0010

Affected Product	RedHat
Severity	Medium
Affected Vulnerability	Use-after-free (CVE-2019-19527)
Description	Use-after-free vulnerability can be exploited by a malicious USB device in the drivers/hid/usbhid/hiddev.c driver in Redhat systems kernel. Redhat released security patch updates addressing this vulnerability and it is highly recommended to apply these fixes at earliest to avoid such circumstances.
Affected Products	Red Hat Enterprise Linux Server - TUS 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2020:4236 https://access.redhat.com/security/cve/CVE-2019-19527

Affected Product	Python
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-26116)
Description	Systems with below python versions contain multiple vulnerabilities where a remote attacker could exploit and cause spoofing, disclose sensitive information and cross-site scripting. This happens when python incorrectly handles certain character and the remote attacker could use this issue to perform CRLF injection.
Affected Products	Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9 3.8.x before 3.8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://python-security.readthedocs.io/vuln/http-header-injection-method.html

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.