Advisory Alert

Alert No: AAA190130 Date: 30-Jan-19 10:33 AM

Security Updates for 30th January 2019

Overview	High	Cisco	▪ Arbitrary Code Execution
		Microsoft Exchange	▪ Privilege Escalation Flaw
	Medium	Red Hat	▪ Systemd: stack overflow Vulnerabilities
		Red Hat	▪ Buffer Overflow Vulnerabilities

Description / Impact

Cisco

- A vulnerability in web-based management interface could allow an authenticated remote attacker to execute arbitrary commands.
- Affected Products: **Cisco Small Business RV320**
  RV325 Dual Gigabit WAN VPN Routers
- Officially Acknowledged by the Vendor: **Yes**

Microsoft Exchange

- A vulnerability in Microsoft Exchange could allow privilege escalation to the Domain admin account.
- Affected Products: **Microsoft Exchange 2013 and newer**
- Officially Acknowledged by the Vendor: **No**

RedHat

- RedHat has released a bug fix for systemd package which could result Stack overflow when calling syslog from a command with long cmdline and when receiving many journald entries.
- Affected Products: **Red Hat Enterprise Linux Server - Extended Update Support 7.5 x86_64**
  Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.5 s390x
  Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.5 ppc64
  Red Hat Enterprise Linux EUS Compute Node 7.5 x86_64
  Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.5 ppc64le
- Officially Acknowledged by the Vendor: **Yes**

RedHat

- RedHat has released a bug fix for kernel-alt packages which could result Heap-based buffer overflow.
- Affected Products: **Red Hat Enterprise Linux for ARM 64 7 aarch64**
  Red Hat Enterprise Linux for Power 9 7 ppc64le
  Red Hat Enterprise Linux for IBM System z (Structure A) 7 s390x
- Officially Acknowledged by the Vendor: **Yes**

Risk Reduction Recommendations

Visit the links below and follow the instructions given by respective vendors.

Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-rv-inject
Microsoft	https://kb.cert.org/vuls/id/465632/
RedHat	https://access.redhat.com/errata/RHSA-2019:0204
RedHat	https://access.redhat.com/errata/RHSA-2019:0162

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.