Security and Proprietary Software

By *Roy Schestowitz*
Created *19/07/2021 - 5:11am*
Submitted by Roy Schestowitz on Monday 19th of July 2021 05:11:06 AM Filed under Security [1]

- **Linux servers are getting a welcome security upgrade [2]**

  Cybersecurity firm Sophos has acquired Linux security vendor Capsule8 in a bid to extend its protection cover to Linux servers.

  Capsule8 offers a threat detection platform for securing Linux production environments across bare-metal and virtualized servers, as well as containers, whether deployed on-premise or in the cloud.

  Acquired for an unknown sum, Sophos intends to integrate Capsule8?s protection platform into its Adaptive Cybersecurity Ecosystem (ACE) platform.

- **Critical Juniper Bug Allows DoS, RCE Against Carrier Networks [3]**

  Telecom providers, including wireless carriers, are at risk of disruption of network service if the bug in SBR Carrier is exploited.

  [...]

  One of these can also be used for RCE, Juniper said. That bug (CVE-2021-0277, with an 8.8 CVSS rating) is an out-of-bounds read vulnerability afflicting Junos OS (versions 12.3, 15.1, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1, 20.2, 20.3 and 20.4), and Junos OS Evolved (all versions).

  Junos OS and Junos OS Evolved are network operating systems that power Juniper?s enterprise routers and switches. The former runs on FreeBSD, while the latter runs a version of Linux.

The issue exists in the processing of specially crafted LLDP frames by the Layer 2 Control Protocol Daemon (l2cpd). LLDP is the protocol that network devices use to broadcast their identity, capabilities and neighbors on a local area network (usually over wired Ethernet).

?Continued receipt and processing of these frames, sent from the local broadcast domain, will repeatedly crash the l2cpd process and sustain the DoS condition,? Juniper said in its advisory, issued Thursday.

In addition to the patch, this bug has a few workarounds. For instance, users can configure a device to not load the l2cpd daemon. However, if it?s disabled, certain protocols (RSTP, MSTP, VSTP, ERP, xSTP and ERP, among others) won?t work.

- **What follows Patch Tuesday? Exploit Wednesday. Grab this bumper batch of security updates from Microsoft ? The Register [4]**

  Microsoft released an XL-sized bundle of security fixes for its products for this month's Patch Tuesday, and other vendors are close behind in issuing updates.

- **SonicWall suggests people unplug their end-of-life gateways under 'active attack' by ransomware crims [5]**

  SonicWall has warned that its older Secure Mobile Access (SMA) 100 series and Secure Remote Access (SRA) gateways are being attacked in the wild by crooks to spread ransomware ? and as some of those devices are end-of-life, don't expect any patches to protect them.

  In an emergency alert on Wednesday, the networking biz said miscreants are "actively targeting" the equipment to, as we understand it, steal credentials from them to compromise networks for "an imminent ransomware campaign."

Security

Source URL: http://www.tuxmachines.org/node/153523

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://www.techradar.com/news/linux-servers-are-getting-a-welcome-security-upgrade
[3] https://threatpost.com/critical-juniper-bug-dos-rce-carrier/167869/
[4] https://www.theregister.com/2021/07/14/patch_tuesday/
[5] https://www.theregister.com/2021/07/15/sonicwall_secure_access/