Version Capability for BGP
draft-abraitis-bgp-version-capability-03

Abstract

In this document, we introduce a new BGP capability that allows the advertisement of a BGP speaker’s version.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 3, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

In modern data center designs, we tend to have conventional hosts participating in the routing process. And the fleet of hosts has different versions of routing daemon. This means that troubleshooting is a crucial part to quickly identify the root cause. This document introduces new BGP capability to advertise the version of routing daemon.

2. Specification of Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Version Capability

The Version Capability is a new BGP capability [RFC5492]. The implementation is specific to the vendor. The version is unstructured and can be defined in any format the vendor decides.

```
+--------------------------------+
|    Version Length (1 octet)    |
+--------------------------------+
|      Version (variable)        |
+--------------------------------+
```

Figure 1

Version Length:

The number of characters in the Version
4. Operation

The Version capability MUST only be used for displaying the version of a speaker in order to make troubleshooting easier. You have a bunch of routers with a number of upstreams each. All of them are with a different operating system and routing daemon installed. Assuming that a specific feature is not working or a bug which is not fixed in an appropriate version, would allow us to quickly identify the pattern which versions are affected. Below is an example of implementation in [FRRouting] how it looks like with version advertised by a BGP sender:

```bash
:~# vtysh -c 'show ip bgp neighbors 198.51.100.1 json' \
> | jq ".198.51.100.1".neighborCapabilities.versions'
{
  "advertisedVersion": "FRRouting 7.2-dev-MyOwnFRRVersion",
  "receivedVersion": "FRRouting 7.2-dev-MyOwnFRRVersion-gc68bb14"
}
```

Figure 2

5. IANA Considerations

IANA maintains the "Border Gateway Protocol (BGP) Parameters" registry with a subregistry called "Capabilities Codes". IANA is requested to assign a capability number from the First Come First Served range for the Version Capability in this document as follows:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>Version Capability</td>
<td>[draft-abraitis-bgp-version-capability]</td>
</tr>
</tbody>
</table>

Table 1: Version Capability

6. Security Considerations

The Version Capability can be treated as sensitive information, thus it would be easier for an attacker to exploit by knowing the specific version of the BGP speaker. This information can be gathered in BGP OPEN messages.
The Version Capability MUST be configurable with a vendor-specific knob to be able to enable or disable the capability. The vendor might implement to disable this capability per neighbor.

It would be safe to enable this for iBGP or inside the same tenant where you have full control and the BGP speaker is behind exit points.

The Version Capability information can be gathered in BGP OPEN messages.

Modifying the information advertised by a router might lead to attacks including bogus software upgrades and also might mask the causes of faults in the network.

Advertising which versions of code and from which vendor it comes may facilitate a number of social-engineering attacks.

Sensitive information leaks can be minimized by using the [RFC5082] mechanism or firewalls to filter out TCP 179 port from untrusted networks. This capability can be disabled per neighbor, thus the sensitive information can’t be disclosed to untrusted neighbors.

7. References

7.1. Normative References

[FRRouting]


7.2. Informative References

Author’s Address

Donatas Abraitis
Hostinger
Jonavos g. 60C
Kaunas 44192
LT

Phone: +370 614 18958
Email: donatas.abraitis@hostinger.com