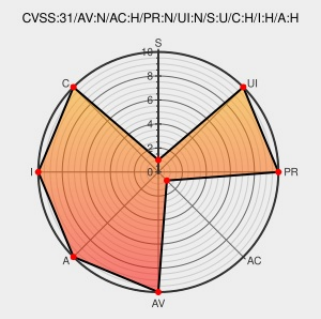
# CVE-2016-5386

Published on: 07/18/2016 12:00:00 AM UTC

Last Modified on: 08/16/2022 01:17:00 PM UTC

## CVE-2016-5386

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Fedora from Fedoraproject contain the following vulnerability:

The net/http package in Go through 1.6 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect CGI applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect a CGI application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue.

CVE-2016-5386 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 8.1 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | HIGH | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 6.8 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Vulnerability Note VU#797896 - CGI web servers assign Proxy header values from | Third Party Advisory<br>US Government Resource | CERT-VN VU#797896 |

| | | |
|---|---|---|
| client requests to internal HTTP_PROXY environment variables | www.kb.cert.org<br>text/html | |
| httpoxy | Third Party Advisory<br>httpoxy.org<br>text/html | MISC httpoxy.org/ |
| Oracle Linux Bulletin - July 2016 | Third Party Advisory<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html |
| [SECURITY] Fedora 24 Update: golang-1.6.3-1.fc24 - package-announce - Fedora Mailing-Lists | Third Party Advisory<br>lists.fedoraproject.org<br>text/html | FEDORA FEDORA-2016-ea5e284d34 |
| Bug 1353798 – CVE-2016-5386 Go: sets environmental variable based on user supplied Proxy request header | Issue Tracking<br>Third Party Advisory<br>bugzilla.redhat.com<br>text/html | CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1353798 |
| [SECURITY] Fedora 23 Update: golang-1.5.4-2.fc23 - package-announce - Fedora Mailing-Lists | Third Party Advisory<br>lists.fedoraproject.org<br>text/html | FEDORA FEDORA-2016-340e361b90 |
| Red Hat Customer Portal | Third Party Advisory<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | REDHAT RHSA-2016:1538 |
| Document Display \| HPE Support Center | h20566.www2.hpe.com<br>text/html | CONFIRM h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03770en_us |
| Oracle Critical Patch Update - July 2017 | www.oracle.com<br>text/html | CONFIRM www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Fedoraproject | Fedora | 23 | All | All | All |
| Operating System | Fedoraproject | Fedora | 24 | All | All | All |
| Operating System | Fedoraproject | Fedora | 23 | All | All | All |
| Operating System | Fedoraproject | Fedora | 24 | All | All | All |
| Application | Golang | Go | All | All | All | All |
| Application | Golang | Go | 1.7 | rc1 | All | All |
| Application | Golang | Go | All | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Oracle | Linux | 7 | All | All | All |
| Operating System | Oracle | Linux | 7 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:*:

cpe:2.3:a:golang:go:*:*:*:*:*:*:*:*:

cpe:2.3:a:golang:go:1.7:rc1:*:*:*:*:*:*:

cpe:2.3:a:golang:go:*:*:*:*:*:*:*:*:

cpe:2.3:o:oracle:linux:7:*:*:*:*:*:*:*:

cpe:2.3:o:oracle:linux:7:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**