Mitigate Microsoft vulnerability MS15-034 and CVE-2015-1635

Use Case:

While doing load balancing we have an opportunity to mitigate vulnerabilities and issues with backend infrastructure. Many data centers run with Microsoft servers and given vulnerabilities can be mitigated on the load balancer while we process the request and parse them for specific patterns.

F5 iRules:

```
################################################
# Name: stop_range_CVE-2015-1635
# Description: This iRule will remove the Range header when
detecting large ranges in it.
################################################
when HTTP_REQUEST {
    # remove Range requests for CVE-2015-1635 if the request uses large ranges
    if { ([HTTP::header exists "Range"]) and ([HTTP::header "Range"] matches_regex
    {bytes\s*=.*([0-9]){10,}.*})}
    {
        HTTP::header remove Range
    }
}
```

URL: https://devcentral.f5.com/articles/using-irules-to-mitigate-microsofts-ms15-034-cve-2015-1635-range-vulnerability

NetScaler Solution:

```
add rewrite action action_stop_range_CVE-2015-1635
delete_http_header Range


add rewrite policy policy_stop_range_CVE-2015-1635
'HTTP.REQ.HEADER("Range").EXISTS &&
HTTP.REQ.HEADER("Range").REGEX_MATCH(re!bytes\s*=.*[0-9]{10,}!)'
action_stop_range_CVE-2015-1635
```

Bind Rewrite policy to VSERVER or to Global rewrite bind point on Response flow. Here using the Rewrite module we are parsing the requests and looking for specific attack pattern. If the pattern is found then the action will delete the Range header from request before sending it to backend server.