1. Object
   1. area\_code: null
   2. asn: "AS15169"
   3. city: null
   4. country\_code: "US"
   5. country\_code3: null
   6. country\_name: "United States"
   7. data: Array(2)
      1. 0:
         1. asn: "AS15169"
         2. cpe: ["cpe:/a:apache:http\_server:2.4.29"]
         3. data: "HTTP/1.1 200 OK
         4. ↵Date: Mon, 27 Jul 2020 10:19:42 GMT
         5. ↵Server: Apache/2.4.29 (Ubuntu)
         6. ↵Last-Modified: Wed, 19 Feb 2020 01:35:48 GMT
         7. ↵ETag: "aa0-59ee3ced0f14b"
         8. ↵Accept-Ranges: bytes
         9. ↵Content-Length: 2720
         10. ↵Vary: Accept-Encoding
         11. ↵Content-Type: text/html
         12. ↵
         13. ↵"
         14. domains: ["googleusercontent.com"]
         15. hash: 1034360746
         16. hostnames: ["177.144.201.35.bc.googleusercontent.com"]
         17. http: {html\_hash: 1148128710, robots\_hash: null, redirects: Array(0), securitytxt: null, title: "403", …}
         18. info: "(Ubuntu)"
         19. ip: 600412337
         20. ip\_str: "35.201.144.177"
         21. isp: "Google Cloud"
         22. location: {city: null, region\_code: null, area\_code: null, longitude: 105, country\_code3: null, …}
         23. opts: {}
         24. org: "Google Cloud"
         25. os: null
         26. port: 80
         27. product: "Apache httpd"
         28. tags: Array(1)
             1. 0: "cloud"
             2. length: 1
             3. \_\_proto\_\_: Array(0)
         29. timestamp: "2020-07-27T10:19:43.129121"
         30. transport: "tcp"
         31. version: "2.4.29"
         32. vulns:
             1. CVE-2017-15710:

cvss: "5.0"

references: (15) ["http://www.openwall.com/lists/oss-security/2018/03/24/8", "http://www.securityfocus.com/bid/103512", "http://www.securitytracker.com/id/1040569", "https://access.redhat.com/errata/RHSA-2018:3558", "https://access.redhat.com/errata/RHSA-2019:0366", "https://access.redhat.com/errata/RHSA-2019:0367", "https://httpd.apache.org/security/vulnerabilities\_24.html", "https://lists.apache.org/thread.html/56c2e7cc9deb1…7e80293cde02fcd65286ba@%3Ccvs.httpd.apache.org%3E", "https://lists.debian.org/debian-lts-announce/2018/05/msg00020.html", "https://security.netapp.com/advisory/ntap-20180601-0004/", "https://support.hpe.com/hpsc/doc/public/display?docLocale=en\_US&docId=emr\_na-hpesbux03909en\_us", "https://usn.ubuntu.com/3627-1/", "https://usn.ubuntu.com/3627-2/", "https://usn.ubuntu.com/3937-2/", "https://www.debian.org/security/2018/dsa-4164"]

summary: "In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod\_authnz\_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all."

verified: false

\_\_proto\_\_: Object

* + - * 1. CVE-2017-15715: {references: Array(13), verified: false, cvss: "6.8", summary: "In Apache httpd 2.4.0 to 2.4.29, the expression sp…by matching the trailing portion of the filename."}
        2. CVE-2018-1283: {references: Array(13), verified: false, cvss: "3.5", summary: "In Apache httpd 2.4.0 to 2.4.29, when mod\_session … pass HTTP header fields, per CGI specifications."}
        3. CVE-2018-1301: {references: Array(16), verified: false, cvss: "4.3", summary: "A specially crafted request could have crashed the…s classified as low risk for common server usage."}
        4. CVE-2018-1302: {references: Array(10), verified: false, cvss: "4.3", summary: "When an HTTP/2 stream was destroyed after being ha…de debug builds, so it is classified as low risk."}
        5. CVE-2018-1303: {references: Array(14), verified: false, cvss: "5.0", summary: "A specially crafted HTTP request header could have…ache\_disk is not concerned by this vulnerability."}
        6. CVE-2018-1312: {references: Array(15), verified: false, cvss: "6.8", summary: "In Apache httpd 2.2.0 to 2.4.29, when generating a… across servers by an attacker without detection."}
        7. CVE-2018-1333: {references: Array(9), verified: false, cvss: "5.0", summary: "By specially crafting HTTP/2 requests, workers wou…TP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33)."}
        8. CVE-2018-11763: {references: Array(12), verified: false, cvss: "4.3", summary: "In Apache HTTP Server 2.4.17 to 2.4.34, by sending…ible mitigation is to not enable the h2 protocol."}
        9. CVE-2018-17199: {references: Array(10), verified: false, cvss: "5.0", summary: "In Apache HTTP Server 2.4 release 2.4.37 and prior…xpiry time is loaded when the session is decoded."}
        10. CVE-2019-0196: {references: Array(16), verified: false, cvss: "5.0", summary: "A vulnerability was found in Apache HTTP Server 2.…request and thus process the request incorrectly."}
        11. CVE-2019-0197: {references: Array(10), verified: false, cvss: "4.9", summary: "A vulnerability was found in Apache HTTP Server 2.… set "H2Upgrade on" are unaffected by this issue."}
        12. CVE-2019-0211: {references: Array(33), verified: false, cvss: "7.2", summary: "In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.3…he scoreboard. Non-Unix systems are not affected."}
        13. CVE-2019-0220:

cvss: "5.0"

references: (15) ["http://lists.opensuse.org/opensuse-security-announce/2019-04/msg00051.html", "http://lists.opensuse.org/opensuse-security-announce/2019-04/msg00061.html", "http://lists.opensuse.org/opensuse-security-announce/2019-04/msg00084.html", "http://www.openwall.com/lists/oss-security/2019/04/02/6", "http://www.securityfocus.com/bid/107670", "https://httpd.apache.org/security/vulnerabilities\_24.html", "https://lists.debian.org/debian-lts-announce/2019/04/msg00008.html", "https://lists.fedoraproject.org/archives/list/pack…ect.org/message/ALIR5S3O7NRHEGFMIDMUSYQIZOE4TJJN/", "https://lists.fedoraproject.org/archives/list/pack…ect.org/message/EZRMTEIGZKYFNGIDOTXN3GNEJTLVCYU7/", "https://lists.fedoraproject.org/archives/list/pack…ect.org/message/WETXNQWNQLWHV6XNW6YTO5UGDTIWAQGT/", "https://seclists.org/bugtraq/2019/Apr/5", "https://security.netapp.com/advisory/ntap-20190625-0007/", "https://support.f5.com/csp/article/K44591505", "https://usn.ubuntu.com/3937-1/", "https://www.debian.org/security/2019/dsa-4422"]

summary: "A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them."

verified: false

\_\_proto\_\_: Object

* + - * 1. \_\_proto\_\_: Object
      1. \_shodan:
         1. crawler: "5faf2928ceb560cb4276cc1b4660b2d763cc6397"
         2. id: "f7d99990-8014-4ada-bf2c-e91a5508ca74"
         3. module: "http"
         4. options: {}
         5. ptr: true
         6. \_\_proto\_\_: Object
      2. \_\_proto\_\_: Object
    1. 1: {ip: 600412337, http: {…}, port: 443, transport: "tcp", version: "2.4.29", …}
    2. length: 2
    3. \_\_proto\_\_: Array(0)
  1. dma\_code: null
  2. domains: Array(1)
     1. 0: "googleusercontent.com"
     2. length: 1
     3. \_\_proto\_\_: Array(0)
  3. hostnames: Array(1)
     1. 0: "177.144.201.35.bc.googleusercontent.com"
     2. length: 1
     3. \_\_proto\_\_: Array(0)
  4. ip: 600412337
  5. ip\_str: "35.201.144.177"
  6. isp: "Google Cloud"
  7. last\_update: "2020-07-27T10:19:43.129121"
  8. latitude: 35
  9. longitude: 105
  10. org: "Google Cloud"
  11. os: null
  12. ports: Array(2)
      1. 0: 80
      2. 1: 443
      3. length: 2
      4. \_\_proto\_\_: Array(0)
  13. postal\_code: null
  14. region\_code: null
  15. tags: ["cloud"]
  16. vulns: Array(14)
      1. 0: "CVE-2019-0220"
      2. 1: "CVE-2019-0197"
      3. 2: "CVE-2019-0196"
      4. 3: "CVE-2018-1302"
      5. 4: "CVE-2019-0211"
      6. 5: "CVE-2017-15710"
      7. 6: "CVE-2018-1301"
      8. 7: "CVE-2018-1283"
      9. 8: "CVE-2018-1303"
      10. 9: "CVE-2017-15715"
      11. 10: "CVE-2018-1333"
      12. 11: "CVE-2018-17199"
      13. 12: "CVE-2018-11763"
      14. 13: "CVE-2018-1312"
      15. length: 14
      16. \_\_proto\_\_: Array(0)
  17. \_\_proto\_\_: Object