






Subject: [Fail2Ban] swissmakers-apache-global: Banned 35.216.139.120 from rlinfp02.swissmakers.corp
Date: Sunday, 2 February 2025 at 18:43:25 Central European Standard Time
From: Noreply - Swissmakers GmbH
To: Administration - Swissmakers GmbH



Security Alert from Fail2Ban-UI

A new IP has been banned due to excessive failed login attempts.

-  **Banned IP:** 35.216.139.120
-  **Jail Name:** swissmakers-apache-global
-  **Hostname:** rlinfp02.swissmakers.corp
-  **Failed Attempts:** 1
-  **Country:** CH

More Information about Attacker:

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
```

NetRange: 35.208.0.0 - 35.247.255.255
CIDR: 35.240.0.0/13, 35.208.0.0/12, 35.224.0.0/12
NetName: GOOGLE-CLOUD
NetHandle: NET-35-208-0-0-1
Parent: NET35 (NET-35-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Google LLC (GOOGL-2)
RegDate: 2017-09-29
Updated: 2018-01-24
Comment: *** The IP addresses under this Org-ID are in use by Google Cloud customers ***
Comment:
Comment: Direct all copyright and legal complaints to
Comment: <https://support.google.com/legal/go/report>
Comment:
Comment: Direct all spam and abuse complaints to
Comment: https://support.google.com/code/go/gce_abuse_report
Comment:
Comment: For fastest response, use the relevant forms above.
Comment:
Comment: Complaints can also be sent to the GC Abuse desk
Comment: (google-cloud-compliance@google.com)
Comment: but may have longer turnaround times.
Ref: <https://rdap.arin.net/registry/ip/35.208.0.0>

OrgName: Google LLC
OrgId: GOOGL-2
Address: 1600 Amphitheatre Parkway
City: Mountain View
StateProv: CA
PostalCode: 94043
Country: US
RegDate: 2006-09-29
Updated: 2019-11-01
Comment: *** The IP addresses under this Org-ID are in use by Google Cloud customers ***
Comment:
Comment: Direct all copyright and legal complaints to
Comment: <https://support.google.com/legal/go/report>
Comment:
Comment: Direct all spam and abuse complaints to
Comment: https://support.google.com/code/go/gce_abuse_report
Comment:
Comment: For fastest response, use the relevant forms above.
Comment:
Comment: Complaints can also be sent to the GC Abuse desk
Comment: (google-cloud-compliance@google.com)
Comment: but may have longer turnaround times.
Comment:
Comment: Complaints sent to any other POC will be ignored.
Ref: <https://rdap.arin.net/registry/entity/GOOGL-2>

OrgNOCHandle: GCABU-ARIN
OrgNOCName: GC Abuse
OrgNOCPhone: +1-650-253-0000
OrgNOCEmail: google-cloud-compliance@google.com
OrgNOCRef: <https://rdap.arin.net/registry/entity/GCABU-ARIN>

OrgTechHandle: ZG39-ARIN
OrgTechName: Google LLC
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com

```
OrgTechRef: https://rdap.arin.net/registry/entity/ZG39-ARIN

OrgAbuseHandle: GCABU-ARIN
OrgAbuseName: GC Abuse
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: google-cloud-compliance@google.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/GCABU-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
```

Server Log Entries:

```
77.74.99.12 35.216.139.120 - - [02/Feb/2025:18:43:19 +0100] "GET
/info.php HTTP/1.1" 301 229 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
10.15; rv:103.0) Gecko/20100101 Firefox/103.0 abuse.xmco.fr"
77.74.99.12 35.216.139.120 - - [02/Feb/2025:18:43:19 +0100] "GET
/telescope/requests HTTP/1.1" 301 229 "-" "Mozilla/5.0 (Macintosh; Intel
Mac OS X 10.15; rv:103.0) Gecko/20100101 Firefox/103.0 abuse.xmco.fr"
77.74.99.12 35.216.139.120 - - [02/Feb/2025:18:43:18 +0100] "GET /.env
HTTP/1.1" 301 229 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:103.0) Gecko/20100101 Firefox/103.0 abuse.xmco.fr"
77.74.99.12 35.216.139.120 - - [02/Feb/2025:18:43:16 +0100] "GET /
HTTP/1.1" 301 229 "-" "abuse.xmco.fr"
access.swissmakers.ch 35.216.139.120 - - [02/Feb/2025:18:43:16 +0100]
"GET / HTTP/1.1" 400 226 "-" "-"
```

This email was generated automatically by Fail2Ban.

For security inquiries, contact support@swissmakers.ch

© 2025 Swissmakers GmbH. All rights reserved.