b2evolution CMS 6.11.6 Open Redirection

Authored by Nakul Ratti, Soham Bakore

Posted Feb 10, 2021

b2evolution CMS version 6.11.6 suffers from an open redirection vulnerability.

tags | exploit
advisories | CVE-2020-22840
SHA-256 | c65ab83dc414ae0fd259db2445e3da796cf8cf06d6be4c9e872b07e92bd3283c Download | Favorite | View

Related Files

Change Mirror Download

```
# Exploit Title: *Open redirect in b2evolution CMS 6.11.6 redirect_to
parameter in email_passthrough.php*
# Google Dork: N/A
# Date: 10/02/2021
# Exploit Author: Soham Bakore, Nakul Ratti
# Vendor Homepage: https://b2evolution.net/
# Software Link:
https://b2evolution.net/downloads/6-11-6-stable?download=12405
# Version: 6.11.6
# Tested on: latest version of Chrome, Firefox on Windows and Linux
# CVE : *CVE-2020-22840*

Vulnerable File:
-------------------------
http://host/htsrv/email_passthrough.php <http://host/evoadm.php>

Vulnerable Issue:
-------------------------
redirect_to parameter has no input validation/domain whitelisting.

-------------------------Proof of Concept-----------------------
Steps to Reproduce:

1. Send the following link :
*http://127.0.0.1/htsrv/email_passthrough.php?
email_ID=1&type=link&email_key=5QImTaEHxmAzNYyYvENAtYHsFu7fyotR&redirect_to=http%3A%2F%2Fgoogle.com
<http://127.0.0.1/htsrv/email_passthrough.php?
email_ID=1&type=link&email_key=5QImTaEHxmAzNYyYvENAtYHsFu7fyotR&redirect_to=http%3A%2F%2Fgoogle.com>*
to
the unsuspecting user
2. The user will be redirected to Google.com or any other attacker
controlled domain
3. This can be used to perform malicious phishing campaigns on unsuspecting
users
```


File Archive: December 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	31

Top Authors In Last 30 Days

- Red Hat 150 files
- Ubuntu 68 files
- LiquidWorm 23 files
- Debian 16 files
- malvuln 11 files
- nu11secur1ty 11 files
- Gentoo 9 files
- Google Security Research 6 files
- Julien Ahrens 4 files
- T. Weber 4 files

File Tags

- ActiveX (932)
- Advisory (79,754)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,926)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,602)
- Encryption (2,349)
- Exploit (50,359)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (821)
- Kernel (6,291)
- Local (14,201)
- Magazine (586)
- Overflow (12,419)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,044)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,777)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

File Archives

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

Systems

- AIX (426)
- Apple (1,926)
- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,315)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,469)
- Slackware (941)
- Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed