WordPress UpdraftPlus 1.22.2 Backup Disclosure

Authored by Marc Montpass | Site wordfence.com

Posted Feb 18, 2022

WordPress UpdraftPlus versions 1.16.7 through 1.22.2 suffer from a backup disclosure vulnerability.

tags | advisory, info disclosure
advisories | CVE-2022-0633
SHA-256 | b497726806b3d3cd3a57bcd3b91fab0d6c64ec521a48183b3477b06789862f15

Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
On February 17, 2022, UpdraftPlus, a WordPress plugin with over 3 million installations, updated with a
security fix for a vulnerability discovered by security researcher Marc Montpas. This vulnerability allowed any
logged-in user, including subscriber-level users, to download backups made with the plugin. Backups are a
treasure trove of sensitive information, and frequently include configuration files which can be used to access
the site database as well as the contents of the database itself.

As with all newly reported vulnerabilities, the Wordfence Threat Intelligence team examined the patch and was
able to create a proof of concept. In addition, we released a firewall rule to block any attackers trying to
exploit this vulnerability.  Wordfence Premium, Care, and Response customers received this rule today, February
17, 2022, while Wordfence Free users will receive this rule after 30 days on March 19, 2022.

This vulnerability was patched in version 1.22.3 of UpdraftPlus, and as such we strongly encourage you to
verify that your site is running the most up to date version of the plugin and updating immediately if it is
not.

Description: Authenticated Backup Download

Affected Plugin: UpdraftPlus

Plugin Slug: updraftplus

Plugin Developer: UpdraftPlus.Com

Affected Versions: 1.16.7 - 1.22.2

CVE ID: CVE-2022-0633

CVSS Score: 8.5(High)

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N

Researcher/s: Marc Montpass

Fully Patched Version: 1.22.3

UpdraftPlus is a popular back-up plugin for WordPress sites and as such it is expected that the plugin would
allow you to download your backups. One of the features that the plugin implemented was the ability to send
back-up download links to an email of the site owner’s choice. Unfortunately, this functionality was insecurely
implemented making it possible for low-level authenticated users like subscribers to craft a valid link that
would allow them to download backup files.

The attack starts with the WordPress heartbeat function. The attacker needs to send a specially crafted
heartbeat request containing a data[updraftplus][updraft_credentialtest_nonce] parameter while a backup is
running. If they are able to time this request to any time while a backup is running, the response will return
the backup nonce required to download that particular backup.

Once the attacker has the backup nonce, they can trigger the maybe_download_backup_from_email function, but in
order to do so successfully they’d need to fool a WordPress feature designed to determine the endpoint the
request is being sent to:

[Pl (https://email.wordfence.com/e3t/Btc/GC+113/cwG7R04/VWmXRT8lSp3sN8RzkRBwqxnbW6tdK5Q4FG9cDN5t-
njf5js6pV3Zsc37CgT1gW4sdTrn1Xrbb2W4q0wp76QJFxXW4NTPFh17vBSPN5p4kpnQS-RHW5l9HZg2Cdvm5W1D8y-
92M5VByW2m974x1NKGQxW7QJysB3B-8PLN24lHQ7mv7NKW6sJkfK15C-
2XW6_lZKr7wcpmxF94xJVhz8YjV6G0gq63X2JCW6JRh2y4FPYLgW98mn9_4PvdbKW2M-
Y1d2zQTMcW52xt9f4ZtH9qN3Z53t0NJjJ6N6XlZKVwmgc5W7wk8vJ7hLnxPW4h6zgj487WwqW3CRNP36MTTq5W6M71jx3FWjlcW7y_9sv4-
nxtxW4zQsXR5t2FJqW2Fr14S7XWgTTVW3LqT1NvHSzN8WdMQ-j5sSlV49fdV5lJf0PVV4G201YJbktN14T6KnBK7wjW89z0pY5KCkRq32271 )
ease (https://email.wordfence.com/e3t/Btc/GC+113/cwG7R04/VWmXRT8lSp3sN8RzkRBwqxnbW6tdK5Q4FG9cDN5t-
njf5js6pV3Zsc37CgT1gW4sdTrn1Xrbb2W4q0wp76QJFxXW4NTPFh17vBSPN5p4kpnQS-RHW5l9HZg2Cdvm5W1D8y-
92M5VByW2m974x1NKGQxW7QJysB3B-8PLN24lHQ7mv7NKW6sJkfK15C-
2XW6_lZKr7wcpmxF94xJVhz8YjV6G0gq63X2JCW6JRh2y4FPYLgW98mn9_4PvdbKW2M-
Y1d2zQTMcW52xt9f4ZtH9qN3Z53t0NJjJ6N6XlZKVwmgc5W7wk8vJ7hLnxPW4h6zgj487WwqW3CRNP36MTTq5W6M71jx3FWjlcW7y_9sv4-
nxtxW4zQsXR5t2FJqW2Fr14S7XWgTTVW3LqT1NvHSzN8WdMQ-j5sSlV49fdV5lJf0PVV4G201YJbktN14T6KnBK7wjW89z0pY5KCkRq32271 )
view the full article here to see this code snippet.
(https://email.wordfence.com/e3t/Btc/GC+113/cwG7R04/VWmXRT8lSp3sN8RzkRBwqxnbW6tdK5Q4FG9cDN5t-nlk3kWGhV1-
WJV7CgFKlW849J8C6Z_x1CW2bs9VY7CqFJgN5KLG2Wgvvn9W61Y4g_69L2VpW2WxpMr7N0nNWW5692T57LmbNjW3tZpWL55Y0VJW22XCcl4YN608
6lCnW82TBj37gy6B8W1pC8B22cFLGrW58bkTm6lP0tHW8m0Hh941JDWQW8710p-7VNsPyW8bfnrX5tbTZWM7mgxZ_3JM0W7pqRHR2CqshjW54-
7Nm7xdttVW8Cz-
q266MJsxW24XZNg7JTzsgW1vxCv675Cgn3W4FfzLv8VMzp4W1Z8fpk2BWbygW10hHBB7LXrqMN53SgMpV7t8qVyZRXH8zyXhl3dpV1 ) ]

The issue is the UpdraftPlus_Options::admin_page() === $pagenow check. This requires that the WordPress
$pagenow global variable be set to options-general.php. Subscribers are typically not allowed to access this
page. However, it is possible to spoof this variable on some server configurations, primarily Apache/modPHP.
Similar to a previous vulnerability in WordPress < 5.5.1 also found by this researcher, it’s possible to send a
request to e.g. wp-admin/admin-post.php/%0A/wp-admin/options-general.php?page=updraftplus.
```

Follow us on Twitter

Subscribe to an RSS Feed

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)

```
While subscribers cannot access options-general.php, they are allowed to access admin-post.php. By sending the
request to this endpoint they can fool the $pagenow check into thinking that the request is to options-
general.php, while WordPress still sees the request as being to an allowed endpoint of admin-post.php.

Once this check has been passed, the attacker will need to provide the backup nonce as well as a type
parameter. Finally, as all backups are indexed by timestamp, the attacker will need to perform a small amount
of brute-forcing. Since the initial attack must occur while a backup is ongoing, the attacker will have a
decent idea of the range of timestamps likely to be used by the backup, so they can send a number of requests
with a timestamp parameter starting some time before the initial heartbeat request and incrementing until they
are successfully able to download the backup.

Conclusion

Successfully exploiting this vulnerability would take a skilled attacker with an active account on the target
system, as well as a large amount of trial and error. As such it is likely only to be used in targeted attacks.
Nonetheless, the consequences of a successful targeted attack are likely to be severe, as they could include
leaked passwords and PII, and in some cases site takeover if the attacker is able to obtain database
credentials from a configuration file and successfully access the site database.

As such we urge all users running the UpdraftPlus plugin to update to the latest version of the plugin, which
is version 1.22.3 as of this writing, as soon as possible, if you have not already done so. While the chances
of being exploited are relatively low, the consequences of a successful exploit would be severe.

Wordfence Premium, Care, and Response customers are protected from any exploits targeting this vulnerability by
a firewall rule as of February 17, 2022, while Wordfence Free users will receive this protection after 30 days
on March 19, 2022.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we
offer Incident Response services via Wordfence Care
(https://email.wordfence.com/e3t/Btc/GC+113/cwG7R04/VWmXRT8lSp3sN8RzkRBwqxnbW6tdK5Q4FG9cDN5t-nk73kWF5V1-
WJV7CgLq5N53D7CYn4fPtW4lZrk78vdBcZW6F4Xpb21H8V2W35XR_Y4_7WYFW3196JL6GRsTzW1P08YB2DCV1mW4HVdCJ4sHnTjW7FkXHN99Znst
1N2BFZsNYndHCW6jbcC438tbzWW3MjQdV2Zp1vxW4sKL9f38n-xdW8h2QLD3b07FSW21F0f61SF7TwW5H1KCV4sq7FBN8dQ1VSd1FN_W3M-
sZ55GFbvqN7H_dBdNXTn6W6vGsd-83ZrDVV3gKbW6T2_pWW1hNGBQ4dWTRg3m221 ) . If you need your site cleaned immediately,
Wordfence Response
(https://email.wordfence.com/e3t/Btc/GC+113/cwG7R04/VWmXRT8lSp3sN8RzkRBwqxnbW6tdK5Q4FG9cDN5t-nkr3kWFpV1-
WJV7CgGTQW6RzFLs6nsfj5W8cMQpL7NrSnbW1Zkdm-
5RZyrkW4mBTn22yKlcPW6pF3cv7gGrgKW5RnH2q3nfbbqW5QsZrV5DvMxFW1GmPBN3jzMQTW1fWT8l7Pgwj1N7lT6cjM69K7W1tqZs21dt2bDW3r
fYnlW312yKf8NcCfjW8x-kK048w0t9N35ZcBBwd9W3W8TxdDK8fwlcZW89RHQn5w-XFNW56fB172F-
Bv3N8Xs4kqqlfPKVHZ7Tr1777mZW8_VQXB95DmwSW3rYx-C5MxW28W8TH58Z8vNFh339ql1 ) offers the same service with 24/7/365
availability and a 1-hour response time. Both these products include hands-on support in case you need further
assistance.

Kudos to Marc Montpass for discovering this vulnerability and responsibly reporting it to the UpdraftPlus team.
```

[Login](#) or [Register](#) to add favorites

Intrusion Detection	(866)	BSD	(370)
Java	(2,888)	CentOS	(55)
JavaScript	(817)	Cisco	(1,917)
Kernel	(6,255)	Debian	(6,620)
Local	(14,173)	Fedora	(1,690)
Magazine	(586)	FreeBSD	(1,242)
Overflow	(12,390)	Gentoo	(4,272)
Perl	(1,417)	HPUX	(878)
PHP	(5,087)	iOS	(330)
Proof of Concept	(2,290)	iPhone	(108)
Protocol	(3,426)	IRIX	(220)
Python	(1,449)	Juniper	(67)
Remote	(30,009)	Linux	(44,118)
Root	(3,496)	Mac OS X	(684)
Ruby	(594)	Mandriva	(3,105)
Scanner	(1,631)	NetBSD	(255)
Security Tool	(7,768)	OpenBSD	(479)
Shell	(3,098)	RedHat	(12,339)
Shellcode	(1,204)	Slackware	(941)
Sniffer	(885)	Solaris	(1,607)
Spoof	(2,165)	SUSE	(1,444)
SQL Injection	(16,089)	Ubuntu	(8,147)
TCP	(2,377)	UNIX	(9,150)
Trojan	(685)	UnixWare	(185)
UDP	(875)	Windows	(6,504)
Virus	(661)	Other	
Vulnerability	(31,104)		
Web	(9,329)		
Whitepaper	(3,728)		
x86	(946)		
XSS	(17,478)		
Other			