Severe Vulnerability Fixed In UpdraftPlus 1.22.3

Updated on February 17, 2022 - Marc Montpas

During an internal audit of the UpdraftPlus plugin, we uncovered an arbitrary backup download vulnerability that could allow low-privileged users like subscribers to download a site's latest backups.

If exploited, the vulnerability could grant attackers access to privileged information from the affected site's database (e.g., usernames and hashed passwords).

We reported the vulnerability to the plugin's authors, and they recently released version 1.22.3 to address it. Forced auto-updates have also been pushed due to the severity of this issue. If your site hasn't already, we strongly recommend that you update to the latest version (1.22.3) and have an established security solution on your site, such as Jetpack Security.

You can find UpdraftPlus' own advisory here.

Details

Plugin Name: UpdraftPlus
Plugin URI: https://wordpress.org/plugins/updraftplus/
Author: https://updraftplus.com/

The Vulnerability

Arbitrary Backup Downloads

Affected versions: Every version between 1.16.7 and 1.22.3 (Free version), and
CVE-ID: CVE-2022-0633
WPVDB ID: d257c28f-3c7e-422b-a5c2-e618ed3c0bf3
CVSSv3.1: 8.5
CWSS: 87.6

The plugin uses custom "nonces" and timestamps to securely identify backups. Given the knowledge of said nonce and timestamp can give someone access to quite a few of the plugin's features, making sure this info is only accessible to those who legitimately need it is crucial.

Unfortunately, as we'll demonstrate, it wasn't the case.

Nonce Leak

The first culprit was located on the UpdraftPlus_Admin::process_status_in_heartbeat method.

```
6142  /**
6143   * Receive Heartbeat data and respond.
6144   *
6145   * Processes data received via a Heartbeat request, and returns additional data to pass back to the fron
6146   *
6147   * @param array $response - Heartbeat response data to pass back to front end.
6148   * @param array $data     - Data received from the front end (unslashed).
6149   */
6150  public function process_status_in_heartbeat($response, $data) {
6151      if (!is_array($response) || empty($data['updraftplus'])) return $response;
6152      try {
6153          $response['updraftplus'] = $this->get_activejobs_list(UpdraftPlus_Manipulation_Functions::wp_uns
6154      } catch (Exception $e) {
6155          $log_message = 'PHP Fatal Exception error ('.get_class($e).') has occurred during get active job
6156          error_log($log_message);
6157          $response['updraftplus'] = array(
6158              'fatal_error' => true,
6159              'fatal_error_message' => $log_message
6160          );
6161      // @codingStandardsIgnoreLine
6162      } catch (Error $e) {
6163          $log_message = 'PHP Fatal error ('.get_class($e).') has occurred during get active job list. Err
6164          error_log($log_message);
6165          $response['updraftplus'] = array(
6166              'fatal_error' => true,
6167              'fatal_error_message' => $log_message
6168          );
6169      }
6170
6171      if (UpdraftPlus_Options::user_can_manage() && isset($data['updraftplus']['updraft_credentialtest_nor
6172          if (!wp_verify_nonce($data['updraftplus']['updraft_credentialtest_nonce'], 'updraftplus-credenti
6173              $response['updraftplus']['updraft_credentialtest_nonce'] = wp_create_nonce('updraftplus-cred
6174          }
6175      }
6176
6177      $response['updraftplus']['time_now'] = get_date_from_gmt(gmdate('Y-m-d H:i:s'), 'D, F j, Y H:i');
```

```
6178
6179        return $response;
6180    }
```

It did not properly ensure that the user sending this heartbeat request was an administrator (e.g. via functions like current_user_can), which was a problem since the first thing this function tries to do is grab the list of active backup jobs via the **get_activejobs_list** method.

An attacker could thus craft a malicious request targeting this heartbeat callback to get access to information about the site's latest backup to date, which will among other things contain a backup's nonce.

Backup Download

There are a few ways to download backups on UpdraftPlus, most of which were properly secured.

```
6198        /**
6199         * Find out if the current request is a backup download request, and proceed with the download if it
6200         */
6201        public function maybe_download_backup_from_email() {
6202            global $pagenow;
6203            if ((!defined('DOING_AJAX') || !DOING_AJAX) && UpdraftPlus_Options::admin_page() === $pagenow &&
6204                $findexes = empty($_REQUEST['findex']) ? array(0) : $_REQUEST['findex'];
6205                $timestamp = empty($_REQUEST['timestamp']) ? '' : $_REQUEST['timestamp'];
6206                $nonce = empty($_REQUEST['nonce']) ? '' : $_REQUEST['nonce'];
6207                $type = empty($_REQUEST['type']) ? '' : $_REQUEST['type'];
6208                if (empty($timestamp) || empty($nonce) || empty($type)) wp_die(__('The download link is brok
6209                $backup_history = UpdraftPlus_Backup_History::get_history();
6210                if (!isset($backup_history[$timestamp]['nonce']) || $backup_history[$timestamp]['nonce'] !==
6211                $this->do_updraft_download_backup($findexes, $type, $timestamp, 2, false, '');
6212                exit; // we don't need anything else but an exit
6213            }
6214        }
6215    }
```

Unfortunately, the UpdraftPlus_Admin::maybe_download_backup_from_email method, which is hooked to admin_init didn't directly validate users' roles either.

While it did apply some checks indirectly, such as checking the **$pagenow** global variable, past research has shown that this variable can contain arbitrary user input. Bad actors could use this endpoint to download file & database backups based on the information they leaked from the aforementioned heartbeat bug.

Timeline

2022-02-14 – Initial contact with UpdraftPlus
2022-02-15 – We send them details about this vulnerability
2022-02-16 – UpdraftPlus 1.22.3 is released, forced auto-updates launched

Conclusion

We recommend that you check which version of the UpdraftPlus plugin your site is using, and if it is within the affected range, update it as soon as possible!

At Jetpack, we work hard to make sure your websites are protected from these types of vulnerabilities. We recommend that you have a security plan for your site that includes malicious file scanning and backups. Jetpack Security is one great WordPress security option to ensure your site and visitors are safe.

Credits

Original researcher: Marc Montpas

Thanks to the rest of the Jetpack Scan team for feedback, help, and corrections.

*This entry was posted in **Vulnerabilities** and tagged **Security**, **Vulnerabilities**. Bookmark the **permalink**.*

Marc Montpas

Marc's interests led him to work in the trenches of cybersecurity for the better part of the last decade, notably at companies like Sucuri and GoDaddy. His journey led him to uncover several high-impact security issues while auditing open-source platforms, like WordPress. He's an avid Hacker Capture The Flag player and loves to hypothesize new attack vectors.

Have a question?

Comments are closed for this article, but we're still here to help! Visit the support forum and we'll be happy to answer any questions.

View support forum

Search

Get news & tips from Jetpack

Enter your email address to follow this blog and receive news and updates from Jetpack!

Email Address

Subscribe

Join 111,174 other followers

Browse by Topic

- Affiliates (1)
- Analytics (6)
- Code snippets (32)
- Contribute (6)
- Customer Stories (6)
- Ecommerce (11)
- Events (5)
- Features (56)
- Grow (11)
- hosting (1)
- Innovate (6)
- Jetpack News (45)
- Learn (64)
- Meet Jetpack (14)
- Performance (21)
- Photos & Videos (9)
- Promotions (2)
- Releases (165)
- Search Engine Optimization (11)
- Security (75)
- Small Business (16)
- Social Media (13)
- Support Stories (3)
- Tips & Tricks (85)
- Uncategorized (5)
- Utilities & Maintenance (4)

Vulnerabilities (17)
Website Design (13)
WordAds (1)
WordCamp (3)

Jetpack

EN

WordPress Plugins

Akismet Anti-spam
Jetpack
Jetpack Boost
Jetpack CRM
Jetpack Protect
Jetpack Search
Jetpack Social
Jetpack VideoPress
VaultPress Backup
WP Super Cache

Partners

Recommended Hosts
For Hosts
For Agencies

Developers

Documentation
Beta Program
Contribute to Jetpack

Legal

Terms of Service
Privacy Policy
GDPR

Help

Knowledge Base
Forums
Security Library
Contact Us
Press

Social

Mobile Apps