BYPASSING SECURITY RESTRICTIONS

THE CASE OF CVE-2018-5955

OWASP
The Open Web Application Security Project
• Adam Nurudini
  CEH, ITIL V3, CCNA, CCNP, CASP, PCI-DSS, BSC-IT

  Lead Security Researcher @ Netwatch Technologies
  Project Consultant, Information Security Architects Ltd
  Member, Cybersecurity Resilience Service Team
  Web Application Penetration Tester
INTRODUCTION

The following presentation describes an unauthenticated action in GitStack that allows a remote attacker to add new users and then trigger remote code execution.

<table>
<thead>
<tr>
<th>CVE-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2018-5955</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the username and password fields to the rest/user/ URI.</td>
</tr>
</tbody>
</table>

Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5955

Vulnerability Disclosed by:
An independent security researcher, Kacper Szurek, reported the vulnerability to Beyond Security's SSD

Vendor response
“Since October 17, 2017, we have tried to contact GitStack many times and have received a response, but have not provided details about the solution or workaround.”
• GitStack is a web application that allows users to set up your own private Git server.
• This means you can create a version control system with no content.
• GitStack makes it easy to keep your server up to date. It is really Git for Windows and is compatible with any other Git client. GitStack is completely free for small teams.
## Impact

### CVSS v3.0 Severity and Metrics:
- **Base Score:** 9.8 CRITICAL
- **Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
- **Impact Score:** 5.9
- **Exploitability Score:** 3.9

### CVSS v2.0 Severity and Metrics:
- **Base Score:** 7.5 HIGH
- **Vector:** (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)
- **Impact Subscore:** 6.4
- **Exploitability Subscore:** 10.0

---

**Attack Vector (AV):** Network  
**Attack Complexity (AC):** Low  
**Privileges Required (PR):** None  
**User Interaction (UI):** None  
**Scope (S):** Unchanged  
**Confidentiality (C):** High  
**Integrity (I):** High  
**Availability (A):** High  

**Access Vector (AV):** Network  
**Access Complexity (AC):** Low  
**Authentication (AU):** None  
**Confidentiality (C):** Partial  
**Integrity (I):** Partial  
**Availability (A):** Partial  

**Additional Information:**
- Allows unauthorized disclosure of information  
- Allows unauthorized modification  
- Allows disruption of service

---

**EXPLOIT AVAILABILITY**

- [https://www.exploit-db.com/exploits/43777/](https://www.exploit-db.com/exploits/43777/)  

UPCLOSE WITH CVE-2018-5955

In vulnerable versions of GitStack, a flaw in Authentication.class.php allows unauthenticated remote code execution since $_SERVER['PHP_AUTH_PW'] is passed directly to an exec function.

```php
header('HTTP/1.0 401 Unauthorized');

// Your GitStack credentials were not entered correctly. Please ask your GitStack administrator to give you a username/password and give you access to this repository. <br />

Note: You have to enter the credentials of a user which has at least read access to your repository. Your GitStack administration panel username/password will not work.

else {
    // try to authenticate
    $authenticated = false;
    $Username = $_SERVER['PHP_AUTH_USER'];
    $password = $_SERVER['PHP_AUTH_PW'];
```
UPCLOSE WITH CVE-2018-5955

To exploit the vulnerability, the repository web interface must be enabled, a repository must exist, and a user must have access to the repository.

Note: A passwd file should be created by GitStack for local user accounts. Default location: C:\GitStack\data\passwdfile.

Once an attacker adds a user to the server, he can enable the web repository feature.
UPCLOSE WITH CVE-2018-5955

Now, an attacker can create a repository from a remote location and prevent others from accessing our new repository. In the repository, an attacker can upload a backdoor and use it to execute code:

1. View users
Use the GET method to directly view the user list of the GitStack repository, and there is an unauthorized access information disclosure vulnerability.

List of users on the Gitstack application (information disclosure vulnerability)
2. Create user

Through the POST method, specifying the username and password can directly add the repository user, and there is any user added vulnerability:
2. Create user

New user (root) created
3. Create a repository arbitrarily
Directly POST a name to create the corresponding project, But CSRF_TOKEN is required in POST data. CSRF_TOKEN is obtained as follows, visit the landing page, such as http://$IP/registration/login/?next=/gitstack/ view the source code:

```
<form method="post" action="/registration/login/"
<input type="hidden" name="csrfmiddlewaretoken" value="b0WB6ik2hvhjPsdxM683tvTHGCJeF" />

<br>

<default username/password: admin/admin
```

UPCLOSE WITH CVE-2018-5955

3. Create a repository arbitrarily

Repository name
UPCLOSE WITH CVE-2018-5955

4. Add user to any repository
You can add it by following this format:
POST http://$IP/rest/repository/"repository name"/user/"user name"/

Remote command execution vulnerability
By default, the GitStack Web Interface is enabled. Access http://xx/web/index.php

An unauthenticated user can upload reverse shell payload to the gitstack repository to compromise the web application and the server hosting it.
PROACTIVE REMEDIATION

Focus on development best practices like OWASP Top 10 Application Security Risks – 2017

In this scenario the presenter believes
A2:2017 Broken Authentication
A5:2017 Broken Access Control
A6:2017 Security Misconfiguration