SQL injection vulnerability in Talariax sendQuick Alertplus server admin version 4.3 (CVE-2021-26795)

From: refabrik sec <refabriksec () gmail com>
Date: Thu, 11 Nov 2021 10:22:17 +0800

```
Dear Full Disclosure Team,

We are writing to submit a full disclosure for the following vulnerability
discovered for product Talariax sendQuick Alertplus server admin version
4.3. This is an updated reference for
https://seclists.org/fulldisclosure/2021/Oct/1.

-------------------------------------------------------------------------
*Title:* SQL injection vulnerability in Talariax sendQuick Alertplus server
admin version 4.3

*CVE Reference:* **RESERVED** CVE-2021-26795
*Product:* Talariax sendQuick Alertplus server admin
*Vendor:* TalariaX Pte Ltd
*Vulnerable version: *Talariax sendQuick Alertplus Server Admin version 4.3
Patch no 8HF8 and below.
*Fixed version: *Patch no 8HF11
*Impact: *High
*Vulnerability Type:* SQL Injection (CWE-89)
*Vendor notification (and approval for disclosure):* 2021-Oct-05
*Public Disclosure:* 2021-Oct-06
*Discoverer: *Jerry Toh (t.ghimhong () gmail com), Edmund Ong (
edmund.okx () gmail com)

-------------------------------------------------------------------------

*Vulnerability details: *

SQL Injection in the web interface of Talariax sendQuick Alertplus server
admin allows an authenticated user to perform error-based SQL injection via
unsanitized form fields.

The affected URL is found in the Roster Management function:
/appliance/shiftmgn.php

The attached screenshots (see evidence*.jpeg) shows that:
(1) Vulnerability was discovered showing that there is an error message
which states that the SQL Syntax error after a single quotation mark was
appended upon the form submission causing an error message which is thrown
from the database
(2) Finding was subsequently verified as fixed after input validation was
implemented in the fields.


-------------------------------------------------------------------------

*Proof of concept:*

The following input fields were found to be vulnerable to SQL injection:
Navigate to "Roster Management" > Select Edit Roster > Day Selected > Input
fields "Roster Time". (see evidence-2.jpeg). The screenshot above shows
that there is an error message which states that the SQL Syntax error,
after a single quotation mark ('), is being appended upon the form
submission.

-------------------------------------------------------------------------

*Remediation:*

Although the patch (Patch no 8HF11) was tested to have fixed this, it is
still recommended to use the latest product version/patches. Please
approach the vendor for the latest product patches.

-------------------------------------------------------------------------

*Disclosure details:*
- 2021/10/04 Contacted email for permission to disclose
- 2021/10/05 Vendor responded and approved for public disclosure submission
- 2021/10/06 Public disclosure on SecList (
https://seclists.org/fulldisclosure/2021/Oct/1)
- 2021/11/11 Added CVE details for public disclosure reference

------------------------------------------------------------------------------------
*Additional references:*
Below email attachment is the request approval for disclosure by vendor

Delivered-To: edmund.okx () gmail com
Received: by 2002:a67:c982:0:0:0:0:0 with SMTP id y2csp1780343vsk;
        Mon, 4 Oct 2021 21:31:06 -0700 (PDT)
 (envelope-from <jswong () talariax com>) id 1mXc6V-0004bO-R8; Tue, 05 Oct
2021 12:30:58 +0800
Reply-To: jswong () talariax com
Subject: Re: Responsible disclosure of vulnerability in Talariax sendQuick
Alertplus server admin (patched)
To: Edmund Ong <edmund.okx () gmail com>
Cc: t.ghimhong () gmail com
References: <CAO0qOZwUuMcjpwvdAg1B4vZ-qrWHfwjixaMMTDh2=
11Nr3N47g () mail gmail com>
From: JS Wong <jswong () talariax com>
Organization: TalariaX Pte Ltd
Message-ID: <47e14d24-ee1d-5b06-8f2f-20c7fa586957 () talariax com>
Date: Tue, 5 Oct 2021 12:30:58 +0800
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0)
Gecko/20100101 Thunderbird/78.14.0

--------------DBF6FC3FBFBCBF83D5A5DEEB
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 8bit

Dear Edmund

Hi! Thanks for informing us on the issue found. We are pleased to inform
that we had fixed the issue in our patches and as long as customer
update to the latest patches, the issue is resolved.

If you wish to submit to public domain as CVE, we will not stop you from
doing so.

Thanks for informing us

Regards
```

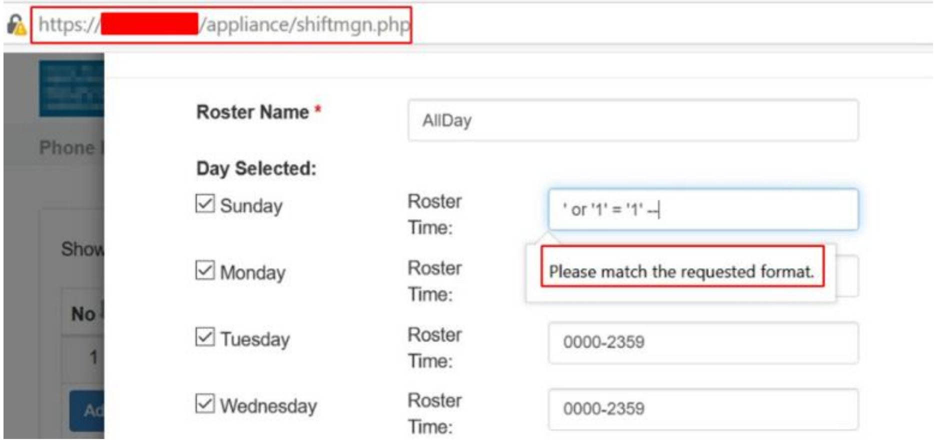
JS

On 4/10/2021 7:24 pm, Edmund Ong wrote:

> Dear Talariax,
>
> We discovered a SQL injection vulnerability on one of your product Talariax sendQuick Alertplus server admin during the period of Q4-2020 to Q1-2021.
>
> This commercial off-the-shelf product was used by one of our clients and they may or may not have reported this to you. The finding was subsequently addressed and finding was closed (as shown in the screenshots the affected patch no 8HF8, and the fix released was patch no 8HF11) although we do not have the specific product version that is affected but we have reason to believe that at that point of testing the product Talariax sendQuick Alertplus server admin version was version 4.3 (do correct us if this is wrong). We felt responsible to share this finding with you directly so that you could ensure this vulnerability would be (or had been) addressed in all subsequent releases.
>
> *Finding details:* SQL Injection in the web interface of Talariax sendQuick Alertplus server admin allows an authenticated user to perform error-based SQL injection via unsanitized form fields.
>
> *Affected URL:* /appliance/shiftmgn.php
>
> *Evidence* (see attached screenshots evidence*.jpeg)
> We attached the following screenshots to evidence that:
> (1) Vulnerability was discovered showing that there is an error message which states that the SQL Syntax error after a single quotation mark was appended upon the form submission causing an error message which is thrown from the database
> (2) Finding was subsequently verified as fixed after input validation was implemented in the fields.
>
> We would also like to seek your approval for us to perform responsible disclosure to the public of this information. The intention is to help potential victims gain knowledge and raise awareness that vulnerability exists, Talariax could also provide us a recommendation if you so please so that we could include in the writeup (e.g. such as to update to the latest patch and versions). Please note that if we don't hear from you within 14 days, we will proceed to do full disclosure through https://nmap.org/mailman/listinfo/fulldisclosure <https://nmap.org/mailman/listinfo/fulldisclosure>.
>
> --
> Yours Sincerely,
> Edmund Ong

--
JS Wong (Mr.)
TalariaX Pte Ltd
76 Playfair Road #08-01 LHK2
Singapore 367996
Tel: +65 62802881 Fax: +65 62806882
Mobile: +65 96367680
Web: http://www.talariax.com

CONFIDENTIALITY NOTE: This email and any files transmitted with it is intended only for the use of the person(s) to whom it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If you are not the intended recipient, please immediately notify the sender and delete the email. If you are not the intended recipient please do not disclose, copy, distribute or take any action in reliance on the contents of this e-mail. Thank you.



https://[redacted]/appliance/shiftmgn.php

Roster Name * AllDay

Day Selected:

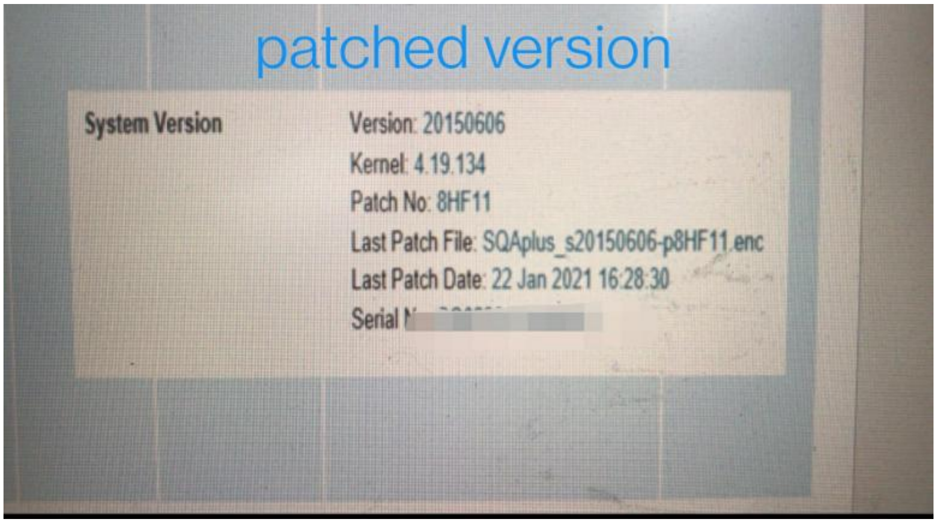
☑ Sunday Roster Time: ' or '1' = '1' --

Please match the requested format.

☑ Monday Roster Time:

☑ Tuesday Roster Time: 0000-2359

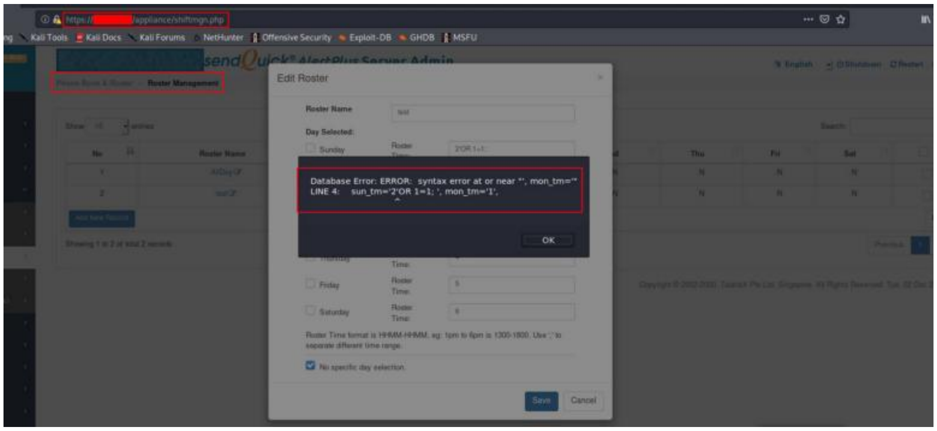
☑ Wednesday Roster Time: 0000-2359



patched version

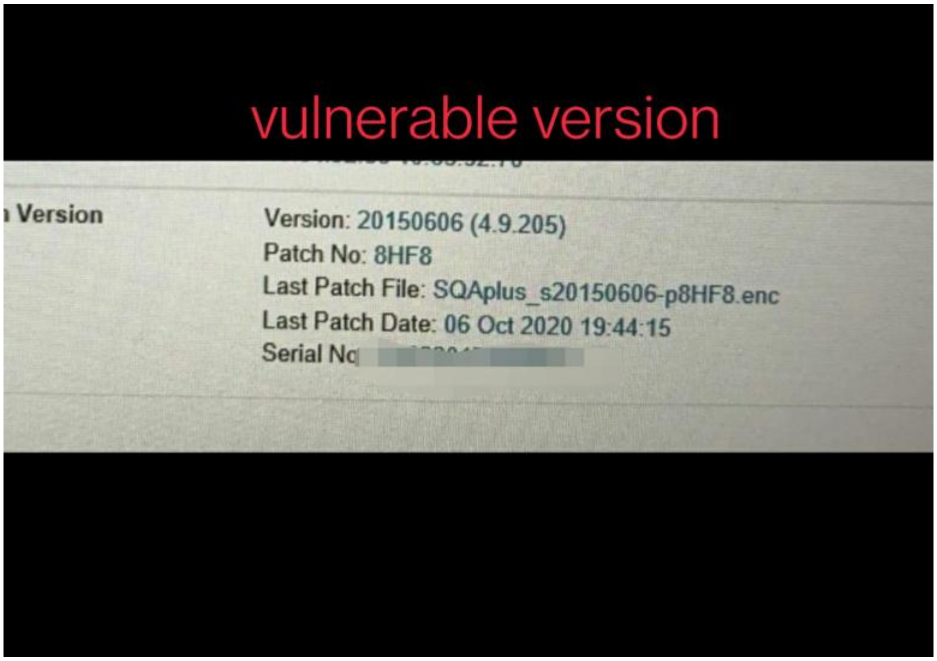
System Version

Version: 20150606
Kernel: 4.19.134
Patch No: 8HF11
Last Patch File: SQAplus_s20150606-p8HF11.enc
Last Patch Date: 22 Jan 2021 16:28:30
Serial N [redacted]



https://[redacted]/appliance/shiftmgn.php

```
Database Error: ERROR:  syntax error at or near "', mon_tm='"
LINE 4:    sun_tm='2'OR 1=1; ', mon_tm='1',
                       ^
```



vulnerable version

Version

Version: 20150606 (4.9.205)
Patch No: 8HF8
Last Patch File: SQAplus_s20150606-p8HF8.enc
Last Patch Date: 06 Oct 2020 19:44:15
Serial No [redacted]

```
_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

- **SQL injection vulnerability in Talariax sendQuick Alertplus server admin version 4.3 (CVE-2021-26795)** *refabrik sec (Nov 12)*