

Talariax sendQuick Alertplus Server Admin 4.3 SQL Injection

Authored by Jerry Toh, Edmund Ong

Posted Nov 15, 2021

Talariax sendQuick Alertplus Server Admin version 4.3 suffers from a vulnerability that allows an authenticated user to perform error-based SQL injection via unsanitized form fields.

tags | exploit, sql injection  
advisories | CVE-2021-26795

SHA-256 | 03baeadadc5e0a514c1a77c9b0a6e994cc7d485726874f0ef7839578d41f5227 Download | Favorite | View

Related Files

Share This

Like Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror

Download

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 (CVE-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 with SMTP id y2csp1780343vsk; Mon, 4 Oct 2021 21:31:06 -0700 (PDT)  
(envelope-from <js Wong@Talariax.com>) id 1mXc6V-0004b0-R8; Tue, 05 Oct 2021 12:30:58 +0800  
Reply-To: js Wong@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: <CA00qQ2WUkCjpwvdAg1B4vZ-grWHFwjxAMMTHz=11Nz3N47g@mail.gmail.com>  
From: JS Wong <js Wong@talariax.com>  
Organization: Talariax Pte Ltd  
Message-ID: <47e14d24-eelid-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

-----DBF6pC3FBPBCBF830SA5ADEEB

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

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11security 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)  
Advisory (79,754)  
Arbitrary (15,694)  
BBS (2,859)  
Bypass (1,619)  
CGI (1,018)  
Code Execution (6,926)  
Conference (673)  
Cracker (840)  
CSRF (3,290)  
DoS (22,602)  
Encryption (2,349)  
Exploit (50,359)  
File Inclusion (4,165)  
File Upload (946)  
Firewall (821)  
Info Disclosure (2,660)  
Intrusion Detection (867)  
Java (2,899)  
JavaScript (821)  
Kernel (6,291)  
Local (14,201)  
Magazine (586)  
Overflow (12,419)  
Perl (1,418)  
PHP (5,093)  
Proof of Concept (2,291)  
Protocol (3,435)  
Python (1,467)  
Remote (30,044)  
Root (3,504)  
Ruby (594)  
Scanner (1,631)  
Security Tool (7,777)  
Shell (3,103)  
Shellcode (1,204)  
Sniffer (886)

File Archives

December 2022  
November 2022  
October 2022  
September 2022  
August 2022  
July 2022  
June 2022  
May 2022  
April 2022  
March 2022  
February 2022  
January 2022  
Older

Systems

AIX (426)  
Apple (1,926)  
BSD (370)  
CentOS (55)  
Cisco (1,917)  
Debian (6,634)  
Fedora (1,600)  
FreeBSD (1,242)  
Gentoo (4,272)  
HPUX (878)  
IOS (330)  
iPhone (108)  
IRIX (220)  
Juniper (67)  
Linux (44,315)  
Mac OS X (684)  
Mandriva (3,105)  
NetBSD (255)  
OpenBSD (479)  
RedHat (12,469)  
Slackware (941)  
Solaris (1,607)

> 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 8HPI1) 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.

Spoof (2,166)	SUSE (1,444)
SQL Injection (16,102)	Ubuntu (8,199)
TCP (2,379)	UNIX (9,159)
Trojan (686)	UnixWare (185)
UDP (676)	Windows (6,511)
Virus (662)	Other
Vulnerability (31,136)	
Web (9,365)	
Whitepaper (3,729)	
x86 (946)	
XSS (17,494)	
Other	

[Login](#) or [Register](#) to add favorites

**packet storm**

© 2022 Packet Storm. All rights reserved.

#### Site Links


News by Month
News Tags
Files by Month
File Tags
File Directory


#### About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

#### Hosting By

Rokasec
---------

 Follow us on Twitter

 Subscribe to an RSS Feed