



CVE-2022-26959

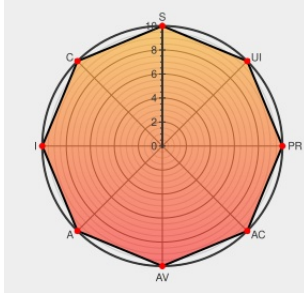
Published on: Not Yet Published

Last Modified on: 09/19/2022 06:25:00 PM UTC

CVE-2022-26959

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AC:L/AV:N/A:H/C:H/I:H/PR:N/S:C/UI:N



Certain versions of [Northstar Club Management](#) from [Globalnorthstar](#) contain the following vulnerability:

There are 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.

CVE-2022-26959 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Threat & Vulnerability Assessment - Assura, Inc.	web.archive.org text/html Inactive Link Not Archived	MISC www.assurainc.com/services/advisory-services/threat-vuln-assessment/
CVE-2022-26959 Northstar Club Management software version 6.3 - Full, Blind/Time-based SQL Injection - Vulnerability Research - Confluence	assura.atlassian.net text/html	MISC assura.atlassian.net/wiki/spaces/VULNS/pages/1842675717/CVE-2022-26959+Northstar+Club+Management+software+version+6.3+-+Full+Blind+Time-based+SQL+Injection

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Globalnorthstar	Northstar Club Management	6.3	All	All	All
cpe:2.3:a:globalnorthstar:northstar_club_management:6.3:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-26959 : There are two full read/write Blind/Time-based SQL injection vulnerabilities in the Northstar Cl... twitter.com/i/web/status/1...	2022-09-16 02:05:32
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-26959 There are two full (read/write) Blind/Time-based SQL injection vu... twitter.com/i/web/status/1...	2022-09-16 02:56:00
 /r/netcve	CVE-2022-26959	2022-09-16 03:38:25

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)