

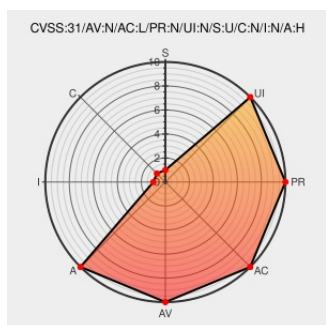


CVE-2021-45918

Published on: Not Yet Published

Last Modified on: 06/26/2023 05:49:00 PM UTC

CVE-2021-45918 - advisory for TVN-202112007

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

Certain versions of [Health Insurance Web Service Component](#) from [Nhi](#) contain the following vulnerability:

NHI's health insurance web service component has insufficient validation for input string length, which can result in heap-based buffer overflow attack. A remote attacker can exploit this vulnerability to flood the memory space reserved for the program, in order to terminate service without authentication, which requires a system restart to

recover service.

CVE-2021-45918 has been assigned by [cve@cert.org.tw](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [NHI](#) - health insurance web service component version = 515BE7DE5BCE446177FEE8A6E0665093

Affected Vendor/Software: [NHI](#) - health insurance web service component version = 42fcc36541e716e23de77d5f325b186a

Affected Vendor/Software: [NHI](#) - health insurance web service component version = 52EACB7CA2B4D0A5A869DF01079BF4D6

Affected Vendor/Software: [NHI](#) - health insurance web service component version = 52EACB7CA2B4D0A5A869DF01079BF4D6

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

TWCERT/CC台灣電腦網路危機處理暨協調中心|企業資安通報協處|資安情資分享|漏洞通報|資安聯盟|資安電子報-健保卡網路服務元件 - Heap-based Buffer Overflow

www.twcert.org.tw

text/html

 MISCwww.twcert.org.tw/tw/cp-132-6227-eaf49-1.html

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	Nhi	Health Insurance Web Service Component	-	All	All	All
cpe:2.3:a:nhi:health_insurance_web_service_component:-:*:*:*:*:*:						

Discovery Credit

Yu-Hsiang Lin

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-45918 : NHI's health insurance web service component has insufficient validation for input string length,... twitter.com/i/web/status/1...	2022-06-20 05:35:23
 /r/netcve	CVE-2021-45918	2022-06-20 06:38:13

[← 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](#)