Path traversal on administrative account in dnnsoftware/dnn.platform

1

Valid Reported on Aug 9th 2022

Description

Relative path traversal in DNN.Platform at log download functionality. Administrative account can download any system file. This could allow direct read access to files that are not meant to be accessible directly by the platform.

Proof of Concept

Login as administrative user. Payload tested on DNN 9.1.1

```
curl -i -s -k -X $'GET' \
    -H $'Host: <HOST>' \
    -b $'.DOTNETNUKE=<ADMIN_SESSION>' \
    $'https://<HOST>/<PATH_TO_DNN>/API/PersonaBar/ServerSettingsLogs/GetLog
```

Replace the *<HOST>*, *<ADMIN_SESSION>* and *<PATH_TO_DNN>* with the appropriate values. *<PATH_TO_DNN>* may include the language selection. Other files than *Windows/win.ini* may be leaked, such as *windows/system32/drivers/etc/hosts*. Adjust the number of "../" depending on the local configuration.

Impact

Arbitrary file read. This could leak sensitive system files or any file present on the system.

Occurrences

C# ServerSettingsLogsController.cs L55

Path.Combine without checks on sensitive characters such as "." Exploit was confirmed on a deployment of DNN 9.1.1.

C# ServerSettingsLogsController.cs L75

Path.Combine without checks on sensitive characters such as "." Exploit was confirmed on a deployment of DNN 9.1.1.

CVE
CVE-2022-2922
(Published)

Vulnerability Type
CWE-23: Relative Path Traversal

Severity
Medium (4.9)

Registry
Other

Affected Version
(? - 9.1.1 - latest]

Visibility
Public

Status
Fixed

Found by

Mihai-Alexandru Bogatu
@ephvuln
unranked

Fixed by

Mitchel Sellers
@mitchelsellers
maintainer

This report was seen 938 times.

We are processing your report and will contact the **dnnsoftware/dnn.platform** team within 24 hours. 4 months ago

We have contacted a member of the **dnnsoftware/dnn.platform** team and are waiting to hear back 4 months ago

We have sent a follow up to the **dnnsoftware/dnn.platform** team. We will try again in 7 days. 3 months ago

We have sent a second follow up to the **dnnsoftware/dnn.platform** team. We will try again in 10 days. 3 months ago

Mitchel Sellers validated this vulnerability 3 months ago

Mihai-Alexandru Bogatu has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **dnnsoftware/dnn.platform** team. We will try again in 7 days. 3 months ago

We have sent a second fix follow up to the **dnnsoftware/dnn.platform** team. We will try again in 10 days. 3 months ago

We have sent a third and final fix follow up to the **dnnsoftware/dnn.platform** team. This report is now considered stale. 3 months ago

Mihai-Alexandru 2 months ago Researcher

Requesting for publication. @admin

Mitchel Sellers 2 months ago Maintainer

We are publishing now!

Mitchel Sellers marked this as fixed in **9.11.0** with commit **9b1735** 2 months ago

Mitchel Sellers has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

ServerSettingsLogsController.cs#L55 has been validated ✔

ServerSettingsLogsController.cs#L75 has been validated ✔

Sign in to join this conversation