2

https://[redacted] Impacted by DNN ImageHandler SSRF

Share:

State	○ Resolved (Closed)
Disclosed	**October 9, 2019 12:13am +0530**
Reported To	**U.S. Dept Of Defense**
Weakness	Server-Side Request Forgery (SSRF)
Severity	Critical (9 ~ 10)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

warsong submitted a report to U.S. Dept Of Defense. Jan 19th (9 months ago)

Summary:

https://[redacted] runs DNN 8.0.0 to 9.1.1 and is impacted by CVE 2017-0929 allowing for a SSRF through the DNN ImageHandler. Origin servers will request any image file supplied by the attacker. This allows for internal NIPR sites to be mapped and accessed through a vulnerable host. The attack is limited by file extension.

Impact

Vulnerable site allows interaction with internal NIPR sites. Pulling default image files from internal NIPR sites verifies the site is online and responsive. Discloses origin IP addresses, and could be manipulated further. This could also be used as a defacement technique making the sight display images of radical ideologies or pornography.

Step-by-step Reproduction Instructions

Access the DNN image handler on the vulnerable site.

Supply Burp collaborator payload (working on free burp right now and cannot provide a collab payload) or external attacker controlled image for SSRF trigger.

Payload Example:

https://[redacted]/DnnImageHandler.ashx?mode=file&url=http://1.bp.blogspot.com/-q19YK-T_wAU/UdpDm76jIgI/AAAAAAAAAWo/yjeRx4Vet80/s400/meme11.jpg

https://[redacted]/DnnImageHandler.ashx?mode=file&url=http://www.xn--4zhaa/data/uploads/images/DC3_seal.png

Product, Version, and Configuration

DNN 8.0.0 to 9.1.1 with ImageHandler exposed.

Suggested Mitigation/Remediation Actions

Upgrade to DNN 9.2.0 or later. If upgrading isn't possible, consider blocking requests to ImageHandler if it is unused.

Impact

Recommend High Severity: Vulnerable site allows interaction with internal NIPR-Only sites. Pulling default image files from internal NIPR sites verifies the site is online and responsive. Discloses origin IP addresses, and could be manipulated further to cause harm on internal NIPR sites. This could also be used as a defacement technique making the sight display images of radical ideologies or pornography.

BOT: U.S. Dept Of Defense posted a comment. Jan 19th (9 months ago)

Greetings from the Department of Defense (DoD),

Thank you for supporting the DoD Vulnerability Disclosure Program (VDP).

By submitting this report, you acknowledge understanding of, and agreement to, the DoD Vulnerability Disclosure Policy as detailed at @DeptofDefense.

The VDP Team will review your report to ensure compliance with the DoD Vulnerability Disclosure Policy. If your report is determined to be out-of-scope, it will be closed without action.

We will attempt to validate in-scope vulnerability reports and may request additional information from you if necessary. We will forward reports with validated vulnerabilities to DoD system owners for their action.

Our goal is to provide you with status updates not less than every two weeks until the reported vulnerability is resolved.

Regards,

The VDP Team

ag3nt-j1 updated the severity to Critical. Jan 22nd (9 months ago)

ag3nt-j1 changed the status to ○ **Triaged**. Jan 22nd (9 months ago)

Greetings,

We have validated the vulnerability you reported and are preparing to forward this report to the affected DoD system owner for resolution.

Thank you for bringing this vulnerability to our attention!

We will endeavor to answer any questions the system owners may have regarding this report; however, there is a possibility we will need to contact you if they require more information to resolve the vulnerability.

You will receive another status update after we have confirmed your report has been resolved by the system owner. If you have any questions, please let me know.

Thanks again for supporting the DoD Vulnerability Disclosure Program.

Regards,

The VDP Team

ag3nt-j1 closed the report and changed the status to ○ **Resolved**. Jan 29th (8 months ago)

Good news!

The vulnerability you reported has been resolved and this report is now closed. If you have any further questions or disagree that the report is resolved, please let us know.

Thank you for your time and effort to improve the security of the DoD information network.

Regards,

The VDP Team

warsong posted a comment. Jan 29th (8 months ago)

Looks good in testing. The ImageHandler actually still 200s but doesn't fetch content. I threw in a collaborator payload and didn't get a DNS lookup or HTTP GET so it looks like it is properly being sanitized.

agent-1 posted a comment. Jan 30th (8 months ago)

Amazing work @warsong. With your permission we'd like to highlight you on our Twitter page @DC3VDP for the month of January. Please let us know if that's okay, and if you have a Twitter handle to tag.

DC3 VDP Team

warsong posted a comment. Jan 31st (8 months ago)

@agent-1 yeah for sure, that would be awesome! I do have a twitter handle but I don't tweet very often. It is @warsong71 but you can also use my name (Lance Cleghorn) if you'd like; thanks for the shoutout!

warsong requested to disclose this report. Feb 7th (8 months ago)

Requesting disclosure on this if your team is amenable to that. Think it would be cool to show the community how awesome at engagement the DC3 team is.

ag3nt-j1 posted a comment. Feb 7th (8 months ago)

I'll get it in the queue Lance, thanks for all you do for us!

agent-1 agreed to disclose this report. Oct 9th (3 days ago)

disclosure approved

This report has been disclosed. Oct 9th (3 days ago)