Gateway information leakage

36

Share:

State	Resolved (Closed)
Disclosed	July 30, 2019 8:12pm +0530
Reported To	U.S. Dept Of Defense
Weakness	Privacy Violation
Severity	High (7 ~ 8.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE · EXPORT

hackerfactor submitted a report to U.S. Dept Of Defense. Aug 10th (2 years ago)

Summary:

Many DoD systems use BlueCoat gateways. These gateways insert unique BlueCoat ids that permit tracking DoD users and gaining insight into the DoD network architecture when DoD users access the Internet.

Description:

I run a popular web service (FotoForensics.com -- it's around 150,000 in the Alexa list of top web sites). My public web site is explicitly for research and gets visitors from all over, including from the DoD. One of the research project collects non-standard HTTP headers. The BlueCoat HTTP headers immediately stood out as non-standard.

Someone with a BlueCoat gateway will have headers that look like:

> POST /upload-file.php HTTP/1.1
> Host: www.fotoforensics.com
> Content-Length: 70869
> Cache-Control: max-age=0
> Origin: http://www.fotoforensics.com
> Upgrade-Insecure-Requests: 1
> User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36
> Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryPaSgeQQ5m6kh7aaZ
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
> Referer: http://www.fotoforensics.com/
> Accept-Language: en-[redacted],en;q=0.8
> [redacted]: [redacted] ([redacted]) SC
> Connection: Keep-Alive
> [redacted]: [redacted]

(This example came from a user at the United States Patent and Trademark Office.)

The id found on the "[redacted]" line is unique to the Bluecoat device; it is not unique to the user. However, if this ID ever shows up at a different network address, then it permits a remote (outside of DoD) system to identify associated network addresses, multiple proxy exits, and potentially non-attributable networks. Similarly, if a single IP address is associated with multiple Bluecoat ids, then it denotes a single exit proxy and identifies the (minimum) number of subnets that use the proxy.

For example:

> [redacted]
> [redacted]
> [redacted]
> [redacted]
> [redacted]

> [redacted]
> [redacted]

My server has seen this one IP address associated with 7 different Bluecoat devices.

> [redacted]
> [redacted]
> [redacted]
> [redacted]

This single bluecoat ID has been linked to four different network addresses.

> [redacted]
> [redacted]

This bluecoat id ([redacted]) is interesting because it has been seen on two very different subnets.

> [redacted]
> [redacted]

This bluecoat ID moved locations: it was seen in[redacted] and in/near [redacted]. (Imagine what it could tell an observer if it were to suddenly appear in [redacted]...)

I have currently collected 243 bluecoat IDs associated with "[redacted]". In addition, I've collected 120 bluecoat IDs from the [redacted] Group, 71 ids from the "Headquarters, [redacted]AISC", and ids from many other government organizations.

For example:

> [redacted]
> [redacted]
> [redacted]
> [redacted]
> [redacted]

This one bluecoat id has been observed with both the Department of the Interior and with [redacted]GS. The first 3 ip addresses have hostnames that say "usgs.gov", but the others either lack hostnames or are from the national parks service (nps.gov). And this one id is from 5 IP addresses that span 4 different subnets.

Impact

DoD uses Bluecoat gateways with unique IDs enabled. The unique IDs are supposed to prevent proxy forwarding loops between Bluecoat devices. However, they permit external observers from (1) determining that a Bluecoat device is in use, (2) tracking the device, and (3) gaining insight into the DoD network architecture.

When combined with user-agent strings and other distinct and unique identifiers, this combination of ID and IP address permits determining who likely works with whom.

(Let me know if you want the full list for DoD bluecoat devices. And if you want them for other [redacted] Gov/Mil groups, let me know.)

Suggested Mitigation/Remediation Actions

It varies by Bluecoat device, but buried in each system's configuration menu is an option to disable the unique ID. These should be disabled everywhere.

BOT: U.S. Dept Of Defense posted a comment. Aug 10th (2 years 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

latyzenhaus changed the status to ○ **Triaged**. Aug 11th (2 years 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

hackerfactor posted a comment. Aug 11th (2 years ago)

Thank you. Let me know what else you need.

latyzenhaus updated the severity to High. Aug 11th (2 years ago)

latyzenhaus updated the severity from High to High. Aug 11th (2 years ago)

hackerfactor posted a comment. Apr 8th (2 years ago)

It's been 8 months. Is there any update on this issue?

ag3nt-j1 changed the status to ○ **Needs more info**. Aug 30th (about 1 year ago)

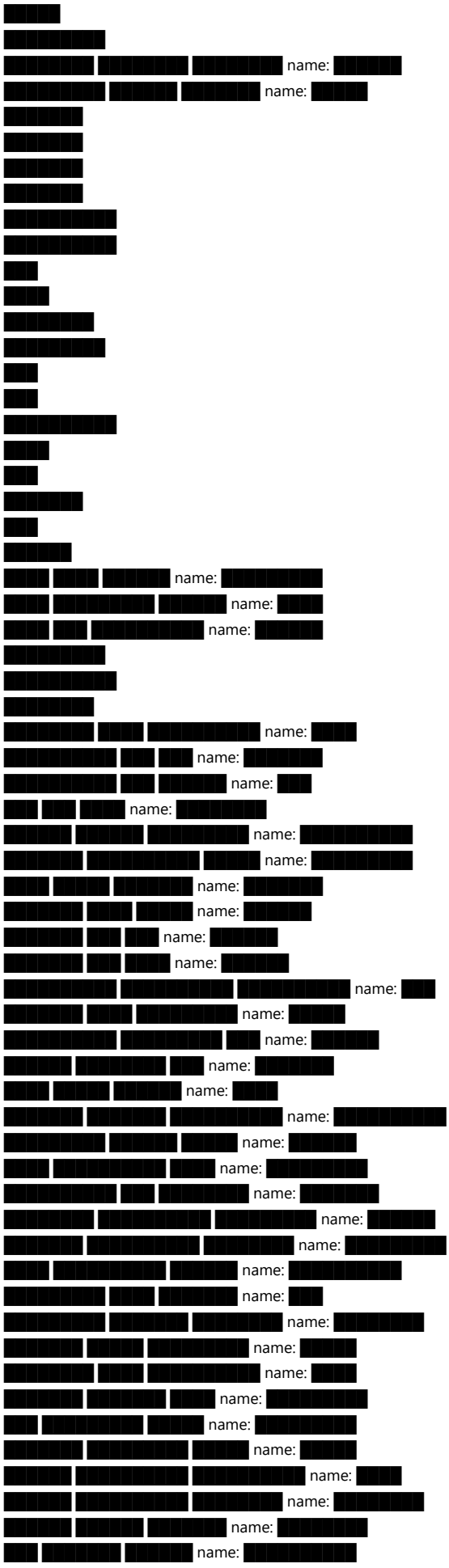
@hackerfactor I'm getting this report back in queue for some validation work. Full disclosure here, this report was filed when a different team were handling things on the technical side here on the program. After reviewing your report I probably would have handled it a little different from our end. As what you have found is a misconfiguration of Bluecoat applicances within the DoD and things like WAFs and loadbalancers tend to fall outside of our scope. And your finding here looks to be an issue at the enterprise level which is also out of our scope. I'm going to need to work with our director to determine how we can push the issue. We tend to process these type of things out as valid and close them as resolved and work them internally due to scope and the impact to how long it takes to address these type of issues...as you can see with the length of time this report has already been opened.

If you can give me a fresh example of this happening and an endpoint I can interact with that would be helpful to try and breath some new life into this report.

hackerfactor changed the status to ○ **New**. Updated Jul 9th (3 months ago)

Hi @ag3nt-j1 -- Thank you for the followup. Here's what my server has seen since 2018-01-01:

> ## IP BluecoatID ASN
>
> [redacted] name: Headquarters, [redacted]AISC
> [redacted]
> [redacted]
> [redacted]
> [redacted]
> [redacted] name: [redacted]
> [redacted]
> [redacted]
> [redacted]



[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted]
[redacted]
[redacted] name: [redacted]
[redacted]
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted]
[redacted]
[redacted] name: [redacted]
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted]
[redacted] name: [redacted]
[redacted]
[redacted]
[redacted]7 name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted]
[redacted] name: [redacted]
[redacted] name: [redacted]
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: Headquarters, [redacted]AISC
[redacted] name: [redacted]

NOTE: This does not include sightings from the DoJ, FBI, [redacted]PTO, or non-gov entities.

Occasionally you'll see the same bluecoat id associated with multiple network addresses (e.g., the last two [redacted] entries) -- that permits determining the network architecture (load balancing exits). And there's a few instances of the same IP with multiple bluecoats behind it (load

balancing internal, one external).

Bluecoat [redacted], [redacted], and [redacted] are really interesting since each spans multiple ASNs.

Beyond this, I can potentially fingerprint browsers. If I were to do this (I'm not, but if I did), then I could estimate the users behind the subnets, work hours, and more.

hackerfactor posted a comment. Sep 1st (about 1 year ago)

You asked for an endpoint to interact with. How about: http://fotoforensics.com/tutorial-malware.php

This is my tutorial on how to detect malware-infected browsers via passive HTTP header inspection. It includes a dump of the HTTP header that your browser sent to my server. If you leak the bluecoat id, it will appear in the list as an HTTP X-Bluecoat-Id header.

ag3nt-j1 posted a comment. Updated Jul 9th (3 months ago)

@hackerfactor thanks for the additional information, love your site by the way. Could have used it a few months ago when I was looking for something to quickly get to exif data rather than the CLI tool in Kali. So your report is unique as you gather the information disclosure from your server logs from DoD and [redacted]G endpoints. We're all back from the holiday weekend here and I will be discussing with the director on how best to address this. As this is a misconfiguration with the Bluecoat from many sites including those within the [redacted]G and DoD I am not real sure how we are going to proceed. Similar issues we've pushed up to an enterprise level for the system owners to make their own determiniations. As this type of finding is outside of our scope there isn't much more we can do. Give me a few days and I'll get a response back to you.

ag3nt-j7 posted a comment. Sep 17th (about 1 year ago)

@ag3nt-j1 ware we keeping this open

hackerfactor posted a comment. Sep 18th (about 1 year ago)

Thanks. Let me know if you need anything else.

deez_nops posted a comment. Dec 19th (10 months ago)

@ag3nt-j1 How do you want to proceed on this report?

hackerfactor posted a comment. Updated Jul 9th (3 months ago)

This bug report was marked as "high" by DoD, and hasn't been acted on in over a year. I don't mind writing it up publicly on my blog. But if you're going to fix it, or send out notices to every impacted group so they can deal with it, then I'll give you more time.

Last I heard (from Sep 17) was that DoD wanted to keep this bug open. However, I haven't seen anything to tell me that the DoD has acted on this issue.

I guess the real question is: How would DoD like to proceed?
A few options:

1. Pay me the bounty and you own the bug.
2. Send notices out to all DoD branches (and preferably all gov sysadmins) and give them time to address it. I can even send you a large list of [redacted] Gov IP-to-Bluecoat mappings.
3. Close it out as no fix and I blog about it. If I blog, I will be very detailed, with IP and bluecoat ID mappings. But I would do DoD as well as lots of foreign nations. E.g., I have a collection of Iranian bluecoat IDs. You can tell when an IP is from an Iranian gov user because they DO NOT have bluecoat IDs. (Iranian citizens go through Bluecoat; Iranian govies do not.)

I'm open to other options, if you have suggestions.

If I blog about it, then lots of admins will learn about it very quickly. Given the time of year, I'd probably blog about it as my 1st or 2nd blog entry of 2019. (IMHO, it's not polite to make everyone panic right before they head off for the holidays.)

How would you like to proceed on this report?

ag3nt-j1 changed the status to ○ **Triaged**. Jan 2nd (9 months ago)

We appreciate your time reporting this vulnerability and the follow up to ensure that it gets mitigated. Although Bluecoats are currently out of scope as they are not DoD websites we have forwarded this to the system owner(s)

and are tracking it to completion. We ask that you please continue to be patient and follow the DoD Vulnerability Disclosure Policy (https://hackerone.com/deptofdefense) on publicly disclosing this prior to receiving written authorization. Once again; very thankful for your submission and your individual efforts to keep our nation's information systems secure. We will provide you with an update once one is received by the system owners.

mrconfidential posted a comment. Jan 5th (9 months ago)

Hey @hackerfactor,

Thank you for participating in the DoD Vulnerability Disclosure Program. My name is Jon Bottarini and I work with the Customer Success team here at HackerOne. It was brought to our attention that you were asking for a bounty for this submission, however **this is not a bug bounty program** where hackers are rewarded with a bounty for their submission.

As highlighted on The Department of Defense's policy, you will need to get written consent in order to publicly disclose the details of any vulnerabilities:

> However, public disclosure of vulnerabilities will only be authorized at the express written consent of DoD.

I apologize for the inconvenience and we hope to see more submissions from you in the future. If you have any questions or concerns about this policy, you can reach out to me here or via my email: jon@hackerone.com

Thank you

hackerfactor posted a comment. Jan 5th (9 months ago)

@ag3nt-j1 Thank you. Just as long as it isn't dropped, I don't mind.

@mrconfidential I didn't realize that it wasn't a bug bounty program. I'll still give them time to inform their people who are vulnerable. However, since they have repeatedly stated that this is out of their scope, I don't see the need to wait for written approval. I'm giving them time as a professional courtesy. But approaching 2 years seems like a lot of time, regardless of the vendor.

ag3nt-j1 changed the status to ○ **Needs more info**. Jan 16th (9 months ago)

@hackerfactor, there has been some movement on your report at the enterprise level and their solution is...interesting. Do you have a larger aggregate of data you could zip up and upload into H1? If we can pin it to enough system owners we are hoping to get bigger eyes on the issue.

hackerfactor changed the status to ○ **New**. Updated Jul 25th (3 months ago)

Hello @ag3nt-j1,

Attached is the list of every bluecoat ID that I've associated with the [redacted] Gov. This list includes direct government groups ([redacted]G) as well as every [redacted], [redacted]GSE, and [redacted]GCTR.

- [redacted]G: Branch of the [redacted] Government
- [redacted]GSE: [redacted] Government Sponsored Entity (effectively [redacted]G)
- [redacted]: [redacted]
- [redacted]GCTR: [redacted] Government Contractor (effectively [redacted]G via oversight and billing)

Only 1 out of 776 records has been manually annotated: the FCC uses AT&T network addresses.

Let me know if you need more info, more details, or have other questions. And if any of the recipients what to know where this data came from, please feel free to identify me and/or my company as the source.

hackerfactor posted a comment. Updated Jul 9th (3 months ago)

Hello @ag3nt-j1,

I found a few more. My search missed an ASN for the United States Coast Guard. I also did a search for any [redacted] Gov-related bluecoat ID has has appeared on any non-Gov networks. This identified some CenturyLink and Level3 addresses. For example:

[redacted]
[redacted]
[redacted]

The same bluecoat device is associated with a DoD network address as well as CenturyLink and Level 3. The new list only shows the non-DoD address, but you can grep the bluecoat ID in the first list and find the Gov network. (I guess I just blew someone's non-attrib network.)

ag3nt-j1 posted a comment. Jan 18th (9 months ago)
Thanks, just finished carving up the data and will be kicking this report over to the next org that needs to address this issue.

ag3nt-j1 changed the status to ○ **Triaged**. Jan 19th (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**. Feb 5th (8 months ago)
@hackerfactor at this point we have distributed the IP list far and wide and at the enterprise level the system owners seem to be taking some action or at least acknowledging the issue. With this being communicated internally I'm hoping that there is enough coverage out there on the issue as well as the IP lists you supplied that this will eventually resolve itself to a degree. We are going to close this out as resolved, I expect any fixes to take some time though.

hackerfactor posted a comment. Updated Jul 9th (3 months ago)
Thank you, @ag3nt-j1. I would like to blog about the vulnerability (not the [redacted] gov portion; I want to call out the some Russian companies, Symantec, Microsoft, and a bunch of others). But I'd like to give the remaining gov groups time to resolve their issues.

Do you think 2 months (April) is enough time?

ag3nt-j1 posted a comment. Updated Jul 9th (3 months ago)
Probably sooner I'd think as this fix will take time to propagate within the DoD and [redacted]G isn't in scope of this program. Though if you want to submit a similar for [redacted]G assests, report to https://www.us-cert.gov/forms/report. I'd suspect it'll take awhile to trickle through the system on that end as well. Let me follow up with you on any additional details, pretty sure if you don't disclose any sensitive info (IPs, hostnames, etc) should be ok but I want to make sure of a few other details. I'm also going to put this report into a disclose status, will take me some time to do the redactions and have the attachments removed...additionally when you blog about this we'd be happy to retweet it over here on the VDP twitter. Give me a week or so, have a few items queued up in the disclose bucket.

ag3nt-j1 requested to disclose this report. Feb 7th (8 months ago)

ag3nt-j1 cancelled the request to disclose this report. Feb 7th (8 months ago)
pending review

hackerfactor posted a comment. Feb 7th (8 months ago)
Thank you. I'll wait. :-)

hackerfactor posted a comment. Jul 8th (3 months ago)
I still haven't received a response about making this public. I would like to make this public either this month (July) or next month (August).

ag3nt-j1 posted a comment. Jul 8th (3 months ago)

I'm going to put in a request to H1 right now to have the attachments and some of the larger bodies of IP and AS numbers redacted. Then I'll go in and touch up as needed before I disclose. You're report (among several others) have been on my list to disclose but had to put the requests on the back burner. Expect this to be completed by the end of the week or earlier. When you make your blog post let us know and we'll tweet it out as well. Sorry to have been keeping waiting on this.

ag3nt-j1 posted a comment. Jul 12th (3 months ago)

@hackerfactor we're ready to disclosure the report. Could you please request the disclosure again in the dropdown?

hackerfactor posted a comment. Updated Jul 25th (3 months ago)

I don't mind the redactions, but it needs to be done consistently. In the initial description's HTTP header, the values for the "[redacted]" and "[redacted]" needs to be redacted. (And I have no idea why you redacted the "Accept-Language" field, but it doesn't matter.)

ag3nt-j1 requested to disclose this report. Jul 30th (2 months ago)

ag3nt-j1 disclosed this report. Jul 30th (2 months ago)