



| Profile |

CVE-2018-6470

P-2025-05-25a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: COMMON VULNERABILITIES & EXPOSURES

May 25, 2023

Created on: April 3, 2023**Intelligence Cut-off:** 12:00 APM (EDT) on May 19, 2023

Profile | CVE-2018-6470

First Observed	February 1, 2018
CVE Dictionary Entry	CVE-2018-6470
NVD Published Date	February 1, 2018
NVD Last Modified	September 8, 2021
Severity	MEDIUM
Base Score	5.3
Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Metasploit Available	No

Current Description

Nibbleblog 4.0.5 on macOS defaults to having .DS_Store in each directory, causing DS_Store information to leak.

RISK

CVE-2018-6470 is an information disclosure vulnerability within Nibbleblog 4.0.5 installed on macOS that creates a .DS_Store file in each Directory. These folders are exposed to the internet via the web service associated with Nibbleblog. Threat actors online have created web crawlers to check for these files. Access to these files can potentially leak sensitive information.

The likelihood of a threat actor leveraging this vulnerability to scan for .DS_Store is High, as the overhead associated with making a script to send simple HTTP requests is so extremely low.

The overall impact of successfully exploiting this vulnerability varies widely depending on the contents within the .DS_Store directory. For this reason, ZeroFox rates the impact of successfully exploiting this vulnerability to be Low.

ZeroFox assesses that the overall risk associated with CVE-2018-6470 is Medium due to the High likelihood of exploitation with the Low impact rating.

| Known Affected Software Configurations

Configuration	Common Platform Enumeration
1	cpe:2.3:a:nibbleblog:nibbleblog:4.0.5:*:*:*:*:*

| Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	NIST

| Summary

CVE-2018-6470 is an unauthenticated information disclosure within Nibbleblog hosted on macOS. This particular vulnerability has been patched for some time, but threat actors displayed suspicious renewed interest in scanning for .DS_store between May 3–9, 2023 (Figure 1). Due to the simple nature of this vulnerability, it is entirely possible that a sensitive .DS_store file could have accidentally been uploaded to a web server through the use of file transfer applications such as rsync, SFTP, et cetera. Locating accidental uploads of .DS_store is likely the reason for the sudden interest by threat actors.

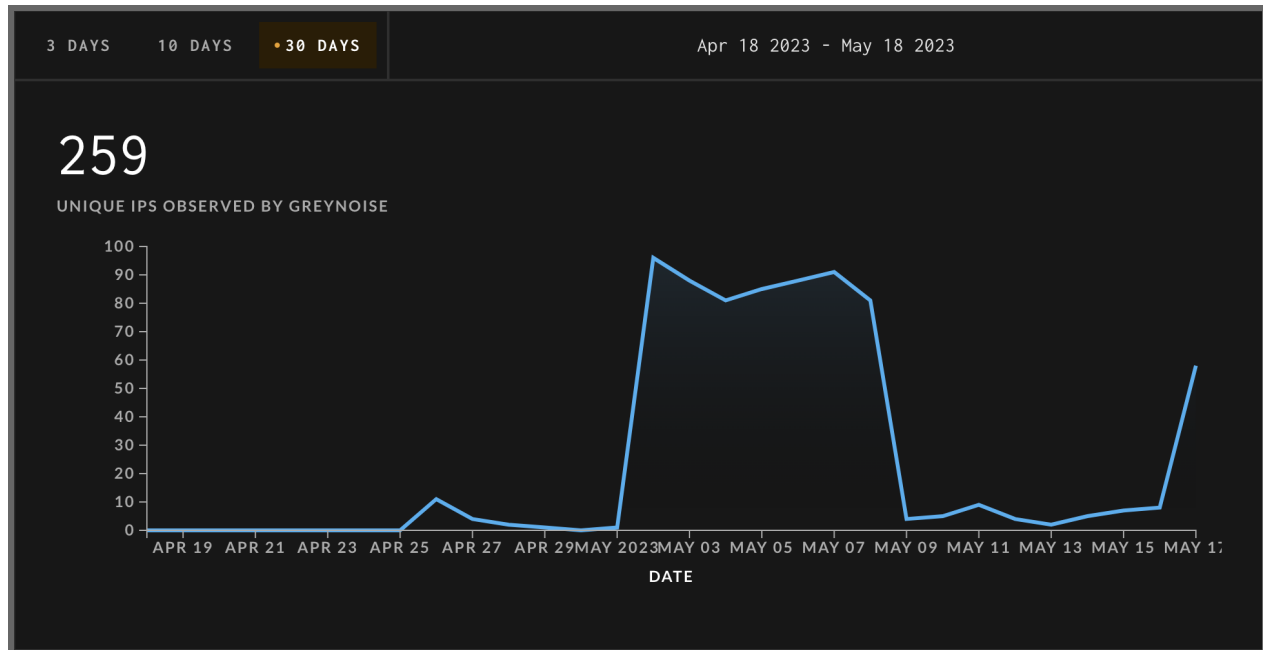


Figure 1. Unique IP Scanning for CVE-2018-6470 Over Time

Source: [hXXps://viz.greynoise\[.\]io/tag/ds-store-scanner?days=30](https://viz.greynoise.io/tag/ds-store-scanner?days=30)

In 2018, a security researcher that goes by the name Sebastian Neef created a .DS_store scanner to locate .DS_store within the Alexa top one million websites.¹ This researcher was able to locate the existence of full document root backups, databases, configuration files, swap/temporary files, and even private keys.

¹ [hXXps://0day\[.\]work/parsing-the-ds_store-file-format/](https://0day[.]work/parsing-the-ds_store-file-format/)

Recommendations

For this particular vulnerability, Sebastian Neef of 0day[.]work provided two different recommendations to mitigate this issue.

1. Deleting .DS_Store from web service directories

```
cd /var/www/ #wherever your web server's document root is
find . -type f -iname "*.DS_Store*"
find . -type f -iname "*DS_Store*" -delete
```

2. Hardening web service to prevent serving .DS_store

```
#Nginx server block
Location ~ /\.DS_Store$ {
    deny all;
}
```

```
#Apache httpd.conf
<Files ~ /\.DS_Store$">
    Order allow,deny
    Deny from all
</Files>
```

| Appendix 1: Indicators of Compromise (Sigma Rules)

```
title: CVE-2018-6470
id: 97786575-c14b-4531-b73a-242d8f60f519
description: Sigma detection rule to detect threat actors scanning for exposed
.DS_Store files that may be hosted on a web server by accident.
status: experimental
date: 2023/5/24
modified: 2023/4/24
author: ZeroFox
tags:
  - mitre.T1595
  - mitre.T1592
  - attack.Reconnaissance
references:
  - https://nvd.nist.gov/vuln/detail/CVE-2018-6470
logsource:
  product: linux
detection:
  accesslog:
    - log.file.path: '*access.log*'
  con:
    event.original:
      - '*.DS_Store*'
  condition: accesslog and con
level: Medium
```

Figure 2. Sigma Rules to detect CVE-2018-6470

Source: ZeroFox Intelligence Collections

| Appendix 2: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.