



FOX

[BLOG](#) // [ADVISORIES](#) // [AUG 17, 2021](#)

eCatcher Desktop, Version 6.6.4 Advisory

By: Priyank Nigam, Senior Security Consultant



Share

eCatcher Advisory Summary

An insecure filesystem permissions vulnerability was identified in eCatcher version 6.6.4 and earlier. To exploit this vulnerability, an attacker must have a user account on the same machine as the victim and have access to the machine during an active VPN connection.

Medium Risk Level Impact

Weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation.

Affected Vendor

Product Vendor	Product Name	Affected Version
Ewon by HMS Networks	eCatcher	Version 6.6.4 and earlier

Product Description:

According to the official product description, eCatcher is a "remote access software that allows remote management of devices within a highly secure environment". The project's official website is <https://www.ewon.biz/technical-support/pages/talk2m/talk2m-tools/talk2m-ecatcher>. The latest version of the application is 6.7.3, released on July 7, 2021.

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).

Accept

Solution

Update to version 6.7.3

VULNERABILITIES

INSECURE FILESYSTEM PERMISSIONS

CVE ID	Security Risk	Impact	Access Vector
CVE-2021-33214	Medium	Escalation of privileges	Local

Files and directories for the eCatcher Talk2MVpnService service have permissions that do not properly enforce access controls. For example, sensitive configuration files are marked as world-writable. Since this service runs under the NT Authority\SYSTEM user, these excessive permissions could lead to privilege escalation on the server.

The directory permissions for the temp directory used by the Talk2MVpnService service were enumerated as follows:

```
PS C:\Users\pn> icacls "C:\Program Files (x86)\eCatcher-Talk2M\Talk2mVpnService\temp"
C:\Program Files (x86)\eCatcher-Talk2M\Talk2mVpnService\temp
BUILTIN\Users:(F)
BUILTIN\Users:(OI)(CI)(IO)(F)
NT SERVICE\TrustedInstaller:(I)(F)
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(I)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
BUILTIN\Administrators:(I)(F)
BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
BUILTIN\Users:(I)(RX)
BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX) APF
```

FIGURE 1 - Full directory access to all users of the system

As highlighted above, all users have full read/write rights over the directory. Since this directory is used to temporarily write OpenVPN configuration files, a user or malware on the system that replaces it successfully could perform privilege escalation when the privileged openvpn process reads it. The **Talk2MVpnService** service recreates this configuration file each time the VPN connection is initiated and prepends the filename with a random UUID, making it unpredictable. Hence, the attack window for exploitation was approximately 15 ms, which made the working exploit unreliable.

Credits

[Privank Nigam](#), Senior Security Consultant, Bishop Fox

Timeline

04/19/2021: Initial discovery
04/30/2021: Contact with vendor
05/12/2021: Vendor acknowledged vulnerabilities
07/07/2021: Vendor released patched version 6.7.3

SUBSCRIBE TO BISHOP FOX'S SECURITY BLOG

Be first to learn about latest tools, advisories,
and findings.

Email Address:

Submit



Priyank Nigam

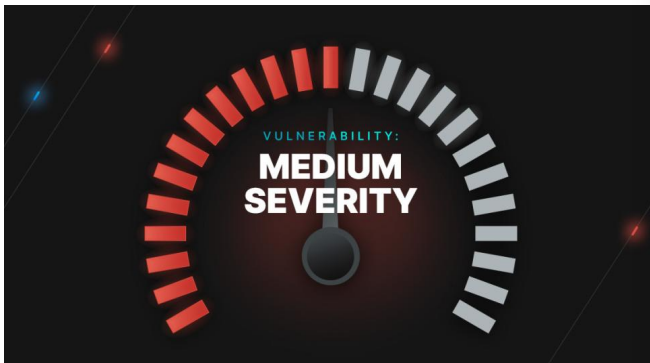
CONSULTANT

(OWASP, GCFE) is a Senior Security Consultant at Bishop Fox. He focuses on web and mobile application penetration testing, and network security. As a researcher, he is interested in all things offensive security, reverse engineering, mobile security, Internet of Things.

[More by Priyank](#)

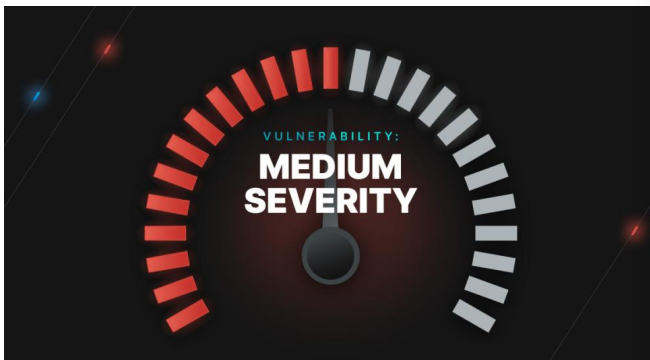
RECOMMENDED POSTS

You might be interested in these related posts.



Dec 15, 2022

FlowscreenComponents Basepack, Version 3.0.7 Advisory



Nov 21, 2022

Log HTTP Requests, Version 1.3.1, Advisory



Oct 24, 2022

Atlassian Jira Align, Version 10.107.4 Advisory



Jul 13, 2022

Netwrix Auditor Advisory

Cosmos Platform

Platform Overview

Attack Surface Management

Exposure Identification

Continuous Attack Emulation

Services

Application Security

Cloud Security

IoT & Product Security

Network Security

Red Team & Readiness

Google, Facebook, & Amazon Partner Assessments

Resources

Resource Center

Blog

Advisories

Tools

Our Customers

Partners

Partner Programs

Partner Directory

Become a Partner

Company

About Us

Careers [We're Hiring](#)

Events

Newsroom

Bishop Fox Mexico

Bishop Fox Labs

Contact Us

This site uses cookies to provide you with a great user experience. By continuing to use our website, you consent to the use of cookies. To find out more about the cookies we use, please see our [Privacy Policy](#).