Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

EventLogCrasher Flaw: Not Serviced by Microsoft

Date of Publication	Admiralty Code	TA Number
February 6, 2023	A1	TA2024044

Summary

First Seen: January 2024
Affected Product: Microsoft Windows
Impact: A recently identified vulnerability, known as EventLogCrasher, poses a significant risk to Windows platforms by allowing authenticated attackers to disrupt the Windows Event Log service. This vulnerability affects all iterations of Windows and has yet to be addressed by Microsoft, lacking an assigned CVE ID.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	MICRO PATCH
Unassigned	Windows EventLogCrasher Vulnerability	Microsoft Windows	✗	✗	✓

Vulnerability Details

#1

A recently discovered vulnerability, dubbed EventLogCrasher, in the Windows platform, allows authenticated attackers to crash the Windows Event Log service. This vulnerability affects all versions of Windows and has been marked as not serviced by Microsoft. A CVE ID has not yet been assigned to this flaw.

#2

The vulnerability stems from the wevtsvc!VerifyUnicodeString routine, which can be accessed via RPC through the ElfrRegisterEventSourceW method. Within the event log service, the wevtsvc!VerifyUnicodeString routine fails to handle a null pointer, leading to an unhandled access violation. Despite the implementation of a null pointer check later in the routine, the flaw persists.

#3 The attack operates through SMB and can be executed by a standard user, proving successful even under default firewall configurations. Upon exploitation, it has the potential to crash the event log service, thereby disrupting log monitoring and potentially suppressing alerts indicating any active security incidents. The Windows Event Log Service auto-restarts after a crash, requiring the attacker to continuously exploit the vulnerability.

#4 Microsoft has designated this vulnerability as not to be serviced and potentially a duplicate of a flaw called LogCrusher, likely from 2022. However, third-party vendors have developed patches for this vulnerability.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
Unassigned	Windows 7 up to the latest Windows 11 and from Server 2008 R2 to Server 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	CWE-476

Recommendations

Network Monitoring: Utilize network monitoring to detect RPC communications and perform anomaly checks to identify any potential issues.

SIEM Log Source Monitoring: Implement SIEM use cases to monitor diverse log sources and generate alerts for any delays or missing logs from a specific source

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	T1059 Command and Scripting Interpreter
T1070 Indicator Removal	T1068 Exploitation for Privilege Escalation	T1040 Network Sniffing	T1211 Exploitation for Defense Evasion
T1078 Valid Accounts	T1210 Exploitation of Remote Services		

References

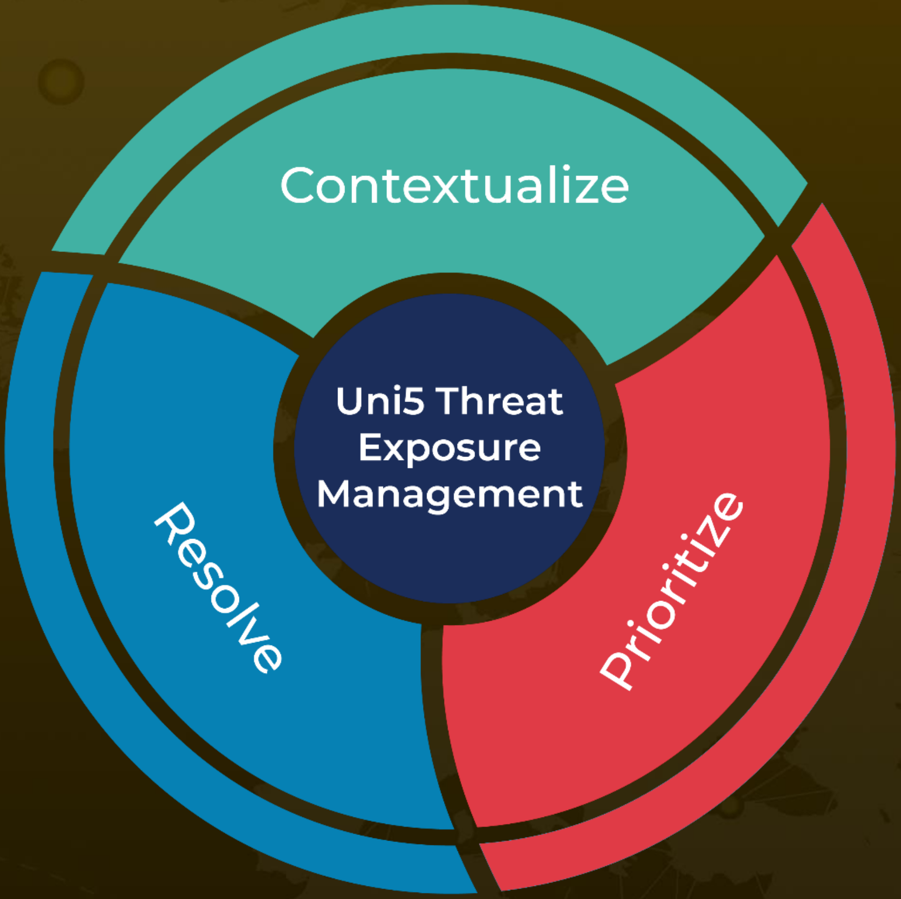
https://blog.0patch.com/2024/01/the-eventlogcrasher-0day-for-remotely.html

https://github.com/floesen/EventLogCrasher

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 6, 2024 • 6:40 AM

More at www.hivepro.com