Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2024-45817: Deadlock Flaw in XenServer and Citrix Hypervisor

Date of Publication	Admiralty Code	TA Number
September 26, 2024	A1	TA2024374

Summary

First Seen: September 24, 2024
Affected Product: XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR
Impact: Citrix has addressed vulnerabilities in XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR, including CVE-2024-45817, which allows malicious administrators of guest VMs to crash or render the host unresponsive. Two additional issues can impact the SNMP service of XenServer 8. Patches and a hotfix (XS82ECU1077) have been released to address these issues, and applying these updates is essential to mitigate risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-45817	XenServer and Citrix Hypervisor Deadlock Vulnerability	XenServer and Citrix Hypervisor	✗	✗	✓
CVE-2022-24805	Net-SNMP Buffer Overflow Vulnerability	XenServer	✗	✗	✓
CVE-2022-24809	Net-SNMP NULL Pointer Dereference Vulnerability	XenServer	✗	✗	✓

Vulnerability Details

#1

Citrix has issued a security bulletin addressing vulnerabilities in XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR (CVE-2024-45817, CVE-2022-24805, CVE-2022-24809). The primary vulnerability, CVE-2024-45817, is related to the x86 Advanced Programmable Interrupt Controller (APIC) architecture, particularly affecting systems running Xen, such as Citrix Hypervisor and XenServer.

#2

The issue arises due to an error in how interrupts are handled by the APIC. Specifically, the vulnerability allows the error interrupt to be configured with an illegal vector, causing recursion in the vlapic_error() function of Xen. When this error interrupt is triggered, the system tries to take a lock recursively, leading to a deadlock.

#3

Although the recursion is bounded, the accumulation of errors in the status register can still create problematic system behavior, rendering it vulnerable to Denial-of-Service (DoS) attacks by crashing or freezing the affected host. Citrix has acknowledged the issue and released security updates for affected versions of Citrix Hypervisor and XenServer. It is recommended to apply these patches to mitigate the risk.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-45817	XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR	cpe:2.3:a:citrix:xenserver:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:hypervisor:*:*:*:*:*:*:*:*	CWE-833
CVE-2022-24805	XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR	cpe:2.3:a:citrix:xenserver:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:hypervisor:*:*:*:*:*:*:*:*	CWE-120
CVE-2022-24809	XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR	cpe:2.3:a:citrix:xenserver:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:hypervisor:*:*:*:*:*:*:*:*	CWE-476

Recommendations

Apply Security Patches Immediately: Review and apply the latest security updates provided by Citrix. Timely application of these patches is crucial to mitigate the risks associated with CVE-2024-45817 and prevent potential exploitation.

Monitor System Logs: Keep an eye on system logs for any error conditions related to APIC and interrupt handling, as this may signal exploitation attempts or system instability.

Restrict Access to Hypervisors: Limit access to the hypervisor, ensuring that only authorized administrators can interact with it. This can reduce the risk of malicious actors configuring illegal interrupt vectors to exploit the vulnerability.

Test in a Controlled Environment: Before applying patches in production environments, thoroughly test them in a sandbox or non-production setup. This will ensure that the patch does not introduce any unintended system behavior.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0040 Impact	TA0042 Resource Development	T1588.005 Exploits
T1499 Endpoint Denial of Service	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1078 Valid Accounts

Patch Links

https://xenbits.xenproject.org/xsa/xsa462.patch

https://support.citrix.com/s/article/CTX691652-hotfix-xs82ecu1077-for-citrix-hypervisor-82-cumulative-update-1

https://github.com/net-snmp/net-snmp/releases/tag/v5.9.4

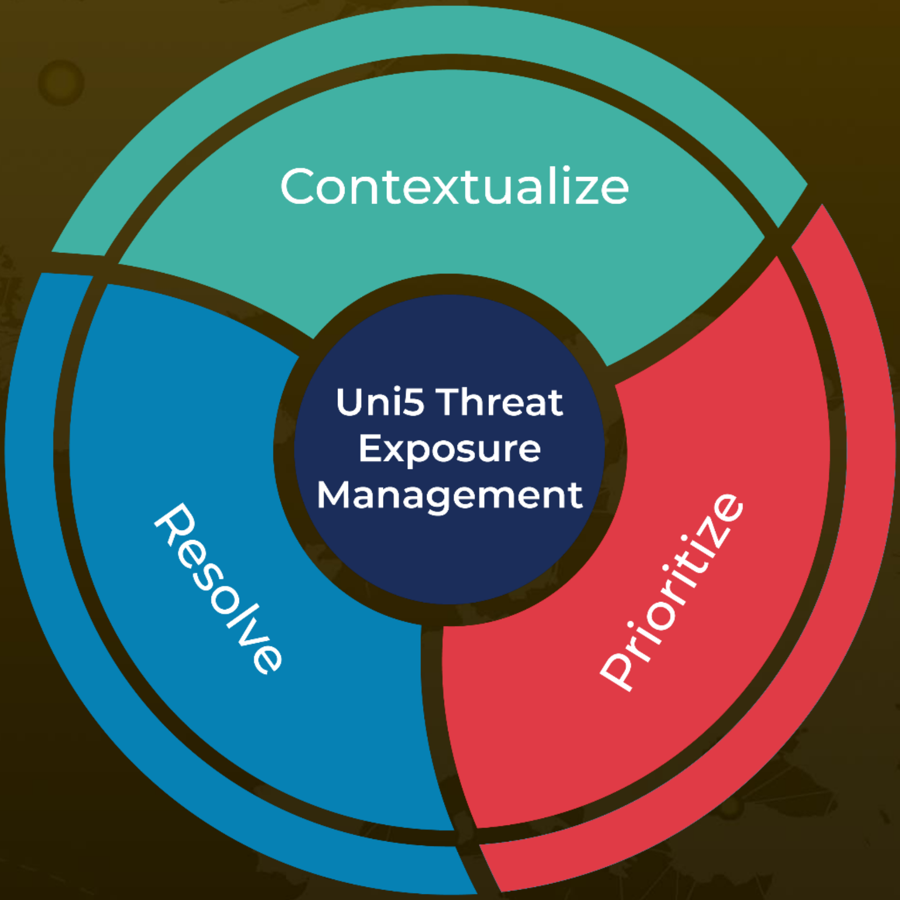
References

https://support.citrix.com/s/article/CTX691646-xenserver-and-citrix-hypervisor-security-update-for-cve202445817

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

September 26, 2024 • 9:30 PM

More at www.hivepro.com