BREAKING CYBERSECURITY NEWS: THREAT ACTOR ALLEGEDLY SELLING VMWARE ESXI 0-DAY EXPLOIT ON HACKER FORUM

Vairav Cyber Security News Report

Date: 2025-02-27

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

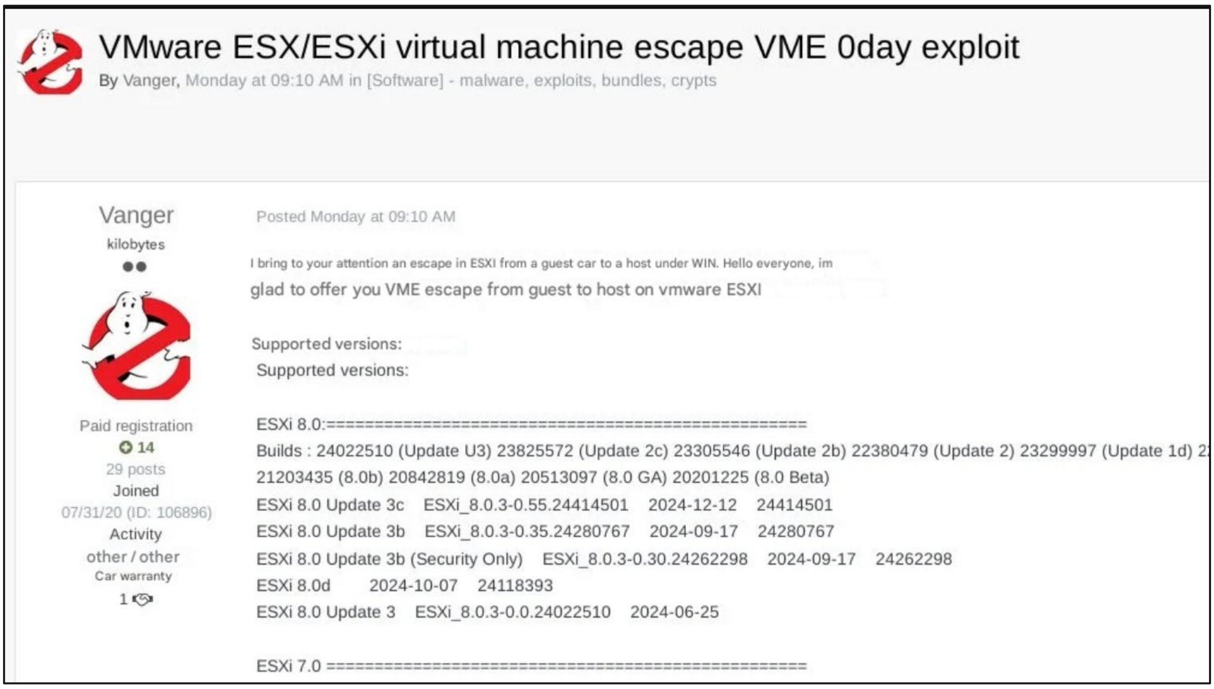
Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A cybercriminal known as "Vanger" has reportedly advertised a zero-day exploit targeting VMware ESXi hypervisors on underground forums. This exploit, priced at $150,000, allegedly enables virtual machine escape (VME), allowing attackers to breach the host system from a guest virtual machine. If authentic, this poses a critical threat to virtualized environments, potentially compromising all virtual machines on a host. Organizations utilizing VMware ESXi are urged to assess their security measures and apply necessary patches promptly.

DETAILS OF THE INCIDENT



VMware ESX/ESXi virtual machine escape VME 0day exploit

By Vanger, Monday at 09:10 AM in [Software] - malware, exploits, bundles, crypts

Vanger
kilobytes
●●

Paid registration
14
29 posts
Joined
07/31/20 (ID: 106896)
Activity
other / other
Car warranty
1

Posted Monday at 09:10 AM

I bring to your attention an escape in ESXI from a guest car to a host under WIN. Hello everyone, im
glad to offer you VME escape from guest to host on vmware ESXI

Supported versions:
Supported versions:

```
ESXi 8.0:===================================================
Builds : 24022510 (Update U3) 23825572 (Update 2c) 23305546 (Update 2b) 22380479 (Update 2) 23299997 (Update 1d) 2
21203435 (8.0b) 20842819 (8.0a) 20513097 (8.0 GA) 20201225 (8.0 Beta)
ESXi 8.0 Update 3c    ESXi_8.0.3-0.55.24414501    2024-12-12    24414501
ESXi 8.0 Update 3b    ESXi_8.0.3-0.35.24280767    2024-09-17    24280767
ESXi 8.0 Update 3b (Security Only)    ESXi_8.0.3-0.30.24262298    2024-09-17    24262298
ESXi 8.0d       2024-10-07    24118393
ESXi 8.0 Update 3    ESXi_8.0.3-0.0.24022510    2024-06-25

ESXi 7.0 ===================================================
```

Figure 1: VMware ESX/ESXi 0 day exploit being sold on Hacker Forum (Translated Post from Russian)

Description of the Cyber Threat: The advertised exploit purportedly affects VMware ESXi versions 5.5 through 8.0, including specific updates up to ESXi 8.0 Update 3c. It claims to enable attackers to escape the isolation provided by the hypervisor, potentially compromising the host operating system and other virtual machines running on the same server. Virtual machine escape vulnerabilities are among the most severe threats to virtualized environments, as they allow attackers to bypass the hypervisor's isolation layer, leading to unauthorized access and control over the host system.

Identification: The exploit was brought to light through a post by "Vanger" on an underground forum, where they offered the zero-day exploit for sale. The seller provided detailed build numbers for the affected VMware ESXi versions, suggesting a comprehensive understanding of the VMware ecosystem. As of now, the authenticity of the exploit remains unverified, and VMware has not released an official statement regarding this specific claim.

Threat Actor: The individual behind this claim operates under the alias "Vanger." Their prior activity appears limited to trading corporate access credentials, with no established reputation for developing or selling exploits. This raises questions about the legitimacy of the exploit, as the underground forums often harbor potential scams.

Affected Entities/Industries: If the exploit is genuine, it could impact a wide range of industries relying on VMware ESXi for virtualization, including financial services, healthcare, manufacturing, government agencies and educational institutions.

Potential Impact: The successful deployment of this exploit could lead to:

- Unauthorized access to sensitive data across multiple virtual machines.
- Operational disruptions due to compromised virtual infrastructure.
- Financial losses stemming from data breaches and system downtimes.
- Reputational damage resulting from public disclosure of security vulnerabilities.

Exploitation Methods: While specific technical details of the exploit have not been disclosed, virtual machine escape vulnerabilities typically involve:

- Exploiting flaws in the hypervisor's code to execute arbitrary commands on the host
- Leveraging vulnerabilities that allow for the escalation of privileges from a guest VM to the host system
- Utilizing crafted inputs or sequences of operations that the hypervisor fails to handle securely

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- **Patch Management**: Ensure all VMware ESXi hypervisors are updated to the latest versions to mitigate known vulnerabilities.
- **Access Control**: Restrict access to ESXi management interfaces to trusted administrators and utilize network segmentation to limit exposure.
- **Service Hardening**: Disable unnecessary services, such as the ESXi Shell and SSH, to reduce potential attack surfaces.

Security Best Practices

- **Regular Audits:** Conduct periodic security assessments of virtual infrastructure to identify and remediate vulnerabilities.
- **Monitoring:** Implement continuous monitoring solutions to detect and respond to suspicious activities on both host and guest systems.
- **Incident Response Planning:** Develop and regularly update incident response plans tailored to virtualization security incidents.

For Advanced Security Teams

- **Threat Intelligence Integration:** Incorporate threat intelligence feeds to stay informed about emerging vulnerabilities and exploits related to virtualization technologies.
- **Behavioral Analysis:** Utilize advanced analytics to detect anomalies indicative of hypervisor compromise or virtual machine escape attempts.
- **Collaboration:** Engage with the cybersecurity community to share insights and gather information on potential threats to virtualization environments.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://cybersecuritynews.com/threat-actor-vmware-esxi-0-day/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com