مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Remote Code Execution Vulnerabilities in Veritas Enterprise Vault

Tracking #:432316544

Date:22-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Veritas has identified multiple critical vulnerabilities in Enterprise Vault, which could allow remote code execution (RCE) through deserialization of untrusted data.

TECHNICAL DETAILS:

Veritas has identified multiple critical vulnerabilities in Enterprise Vault, which could allow remote code execution (RCE) through deserialization of untrusted data. These vulnerabilities affect several versions of the Enterprise Vault server, enabling an attacker to exploit .NET Remoting TCP ports or local IPC services to send specially crafted data to a vulnerable server. Successful exploitation of these vulnerabilities could lead to unauthorized remote code execution, potentially compromising the server and network. Veritas plans to remediate these vulnerabilities in the upcoming Enterprise Vault 15.2 release, but until then, users are advised to follow the recommended mitigation steps to secure their systems.

Vulnerability Details

- **Vulnerability Type**: Deserialization of Untrusted Data Remote Code Execution
- **CVE Identifiers**:
  - ZDI-CAN-24334
  - ZDI-CAN-24336
  - ZDI-CAN-24339
  - ZDI-CAN-24341
  - ZDI-CAN-24343
  - ZDI-CAN-24344
  - ZDI-CAN-24405
- **Severity**: Critical
- **CVSS v3.1 Base Score**: 9.8
- **Vulnerability Description**: On startup, the Enterprise Vault application begins several services that listen on random .NET Remoting TCP ports for commands from client applications. These ports and services are vulnerable due to inherent flaws in .NET Remoting. If an attacker can exploit these services, they can send specially crafted data to the Enterprise Vault server, potentially leading to remote code execution. This attack requires specific conditions, including:
  - **RDP Access**: The attacker must have RDP access to one of the VMs in the network and be part of the Remote Desktop Users group.
  - **Knowledge of the Server**: The attacker needs knowledge of the IP address of the EV server, its process IDs, dynamic TCP ports, and URIs for remoteable objects.
  - **Firewall Misconfiguration**: The firewall on the EV server must be improperly configured to allow access to vulnerable services.

Affected Versions

- **All supported versions of Enterprise Vault**:
  - 15.1, 15.0, 15.0.1, 15.0.2
  - 14.5, 14.5.1
  - 14.4, 14.4.1, 14.4.2
  - 14.3, 14.3.1, 14.3.2
  - 14.2, 14.2.3, 14.2.2, 14.2.1
  - 14.1.3, 14.1.2, 14.1.1, 14.1

- 14.0.1, 14.0

Note: Earlier unsupported versions may also be affected.

Mitigation:
To mitigate the risks posed by these vulnerabilities, Veritas recommends the following actions:

Restrict RDP Access:

- Ensure only trusted users are part of the Remote Desktop Users group and have RDP access to the Enterprise Vault server.
- Limit the RDP access to administrators only, following the guidelines in the Enterprise Vault Administrator's Guide.

Firewall Configuration:

- Ensure that the Enterprise Vault server's firewall is enabled and properly configured to block unauthorized access. The firewall settings should be configured as outlined in the Enterprise Vault Administrator's Guide.

Update Windows Systems:

- Ensure that the latest Windows security updates are installed on the Enterprise Vault server to protect against known vulnerabilities and exploits.

Minimize Access:

- Restrict access to the Enterprise Vault server to only necessary users, reducing the attack surface for potential exploitation.
- Follow best practices for administrator security, ensuring that only trusted and necessary personnel have elevated privileges.

RECOMMENDATIONS:

- Monitor for Suspicious Activity: Continuously monitor the Enterprise Vault server and network for signs of suspicious activity or unauthorized access attempts. Implement intrusion detection systems (IDS) and log monitoring to detect exploitation attempts.
- Prepare for Upcoming Patch: Veritas plans to remediate these vulnerabilities in Enterprise Vault 15.2, with general availability expected in the third quarter of CY25. Users are encouraged to stay updated on this release and apply the patch as soon as it becomes available.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.veritas.com/support/en_US/security/VTS24-014