Security Advisories Relating to Veritas Products

Enterprise Vault Local Elevation of Privilege

March 21, 2013 **SYM13-003**

Revisions

20-April-2016 – Rereleased with Veritas information

Severity

CVSS2 Base Score	Impact	Exploitability	CVSS2 Vector
EV unquoted search path local elevation of privilege - Medium			
6.8	10.0	3.1	AV:L/AC:L/AU:S/C:C/I:C/A:C

Overview

Enterprise Vault (EV) for File System Archiving has an unquoted search path in the File Collector and File PlaceHolder services. This could provide a non-privileged local user the ability to successfully insert arbitrary code in the root path.

Affected Products

Product	Version	Build	Solution
Enterprise Vault for File System Archiving	10.0.0	All	Recommended that users upgrade to 10.0.1 or later
Enterprise Vault for File System Archiving	< 9.0.4	All	Recommended that users upgrade to 9.0.4 or 10.0.1 or later
Enterprise Vault for File System Archiving	8.x	All	Product is EOL/EOS. It is recommended that users upgrade to 9.0.4 or 10.0.1 or later

Products Not Affected

Product	Version
Enterprise Vault for File System Archiving	10.0.1 or later
Enterprise Vault for File System Archiving	9.0.4

Details

Veritas was notified of an unquoted search path issue impacting the File Collector and File PlaceHolder services for Windows deployed as part of Enterprise Vault. This could potentially allow an authorized but non-privileged local user to execute arbitrary code with elevated privileges on the system. A successful attempt would require the local user to be able to insert their code in the system root path undetected by the OS or other security applications where it could potentially be executed during application start-up or reboot. If successful, the local user's code would execute with the elevated privileges of the application.

Veritas Response

This issue was previously identified and fixed as part of Veritas internal testing. The fix was incorporated into versions 10.0.1 and 9.0.4 of Enterprise Vault. Veritas recommends upgrading to the latest version of the software.

Veritas is not aware of exploitation of or adverse customer impact from this issue.

Update Information

Update to latest version (9.0.4; 10.0.1 or later). See Tech Note: TECH54592 for more information

Best Practices

As part of normal best practices, Veritas strongly recommends that customers:

- Restrict access of administration or management systems to privileged users.
- Restrict remote access, if required, to trusted/authorized systems only.
- Run under the principle of least privilege where possible to limit the impact of exploit by threats.
- Keep all operating systems and applications updated with the latest vendor patches.
- Follow a multi-layered approach to security. Run both firewall and anti-malware applications, at a minimum, to provide multiple points of detection and protection to both inbound and outbound threats.
- Deploy network and host-based intrusion detection systems to monitor network traffic for signs of anomalous or suspicious activity. This may aid in detection of attacks or malicious activity related to exploitation of latent vulnerabilities

Credit

Veritas credits Sean McCarthy (http://www.nccgroup.com/) for reporting this issue and working with us.

References

BID: Security Focus, http://www.securityfocus.com, has assigned Bugtraq IDs (BIDs) to these issues for inclusion in the Security Focus vulnerability database.

CVE: These issues are candidates for inclusion in the CVE list (http://cve.mitre.org), which standardizes names for security problems.

CVE	BID	Description
CVE-2013-1609	58617	Enterprise Vault unquoted search path

Disclaimer

THE SECURITY ADVISORY IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Veritas Technologies LLC
500 East Middlefield Road
Mountain View, CA 94043
http://www.Veritas.com

Last modified on: April 20, 2016