Security Advisories Relating to Veritas Products

Enterprise Vault Updates Oracle Outside-In Libraries

September 28, 2012 **SYM12-015**

Revisions

20-April-2016 – Rereleased with Veritas information

Severity

CVSS2 Base Score	Impact	Exploitability	CVSS2 Vector
NBU Management Console Directory Traversal File Download - Medium			
6	6.4	6.8	AV:N/AC:M/Au:S/C:P/I:P/A:P

Overview

Veritas updated the Oracle Outside-In module in the Enterprise Vault product suite. The Oracle Outside-In updates address potential denial of service and possible remote code execution susceptibility.

Affected Products

Product	Version	Build	Solution
Enterprise Vault product suite	10.x and prior	Update to 10.0.2	Enterprise Vault product suite

Details

CERT notified Veritas of vulnerabilities identified in the Oracle Outside-In component. Veritas was already aware of security issues being reported in this module and implemented the updates as soon as it was made available by the vendor.

Oracle's Outside-In module is used by Enterprise Vault product suite to convert data for indexing purposes. These reported issues in Oracle's Outside-In libraries, if successfully exploited, may potentially result in a denial of service in the application or allow the possibility of arbitrary code running in the context of the affected application.

In the Enterprise Vault product suite, attempted exploitation of these issues would require an email with a malicious attachment to be downloaded and stored in a user's mail box until processed for archiving in order to present any potential for malicious activity attempts.

Veritas Response

Veritas has released an update to the Enterprise Vault product suite to address these issues. Veritas recommends all Enterprise Vault product suite customers upgrade to Enterprise Vault 10.0.2 to address any possibility of threats of this nature.

Enterprise Vault 10.0.2 is currently available through normal update channels.

Mitigation

Enterprise Vault product suite enables Data Execution Prevention (DEP) as well as Address Space Layout Randomization (ASLR) in supported versions of Windows to further mitigate successful attempts against these types of issues.

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

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

Will Dormann with CERT.org initially identified these issues to us.

References

http://www.kb.cert.org/vuls/id/118913

Copyright (c) 2016 by Veritas Technologies LLC

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