Security Advisories Relating to Veritas Products

Enterprise Vault Updates Oracle Outside In Module for Multiple Issues

March 5, 2012 **SYM12-004**

Revisions

20-April-2016 – Rereleased with Veritas information

Severity

CVSS2 Base Score	Impact	Exploitability	CVSS2 Vector
Enterprise Vault product suite - Medium			
4.05	6.44	2.69	AV:L/AC:M/Au:S/C:P/I:P/A:P

Overview

Veritas is updating the Oracle Outside In Technology shipped in supported versions of the Enterprise Vault product suite. These Oracle Outside In Technology updates address potential denial of service or code execution susceptibilities

Affected Products

Product	Version	Build	Solution
Enterprise Vault product suite	10.0.x 9.0.x	All	Apply available hot fix (https://www.veritas.com/support/en_US/article.000100435)

Details

Veritas is aware of vulnerabilities identified in the Oracle Outside In Technology libraries, used by Enterprise Vault product suite to convert various types of data for archiving purposes. The issues identified include two issues with parsing of JPEG image files and one with parsing of Lotus 123 v4 files. These issues could potentially result in a denial of service in the application or the possibility of arbitrary code running in the context of the affected application.

Veritas Response

In the Enterprise Vault product suite, attempted exploitation of these issues would require an email with a malicious attachment to be processed locally for archiving to trigger any type of potential exploit attempt.

Enterprise Vault use of the Oracle Outside In technology does not include the conversion of graphics files, which mitigates attack vectors involving graphic file parsing issues. All versions of Enterprise Vault from versions 9.0.3, 10.0 and follow-on releases enable Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) on supporting versions of windows OS. Utilizing DEP and ASLR where supported can aid in mitigation of malicious code in some instances.

Apply available hot fix: https://www.veritas.com/support/en_US/article.000100435

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

Veritas credits Will Dormann with CERT/CC, and an anonymous finder working through TippingPoint's Zero Day Initiative identified these issues to Oracle.

References

http://www.kb.cert.org/vuls/id/738961

http://www.zerodayinitiative.com/advisories/ZDI-12-017/

http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html

Copyright (c) 2016 by Veritas Technologies LLC

Permission to redistribute this alert electronically is granted as long as it is not edited in any way unless authorized by Veritas Product Security. Reprinting the whole or part of this alert in any medium other than electronically requires permission from secure@veritas.com

© 2016 Veritas Technologies LLC. All rights reserved. Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

© 2016 Veritas Technologies LLC. All rights reserved. Veritas and the Veritas Logo are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.