

Veritas InfoScale Operations Manager 8.0.0. Security patch 410

Last updated: 2023-05-03

Legal Notice

Copyright © 2023 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.

This product may contain third-party software for which Veritas is required to provide attribution to the third-party ("Third-Party Programs"). Some of the Third-Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third-party legal notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION 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 TECHNOLOGIES LLC 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.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054
<http://www.veritas.com>

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

CustomerCare@veritas.com

Japan

CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

infoscaledocs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Security patch 8.0.0.410

This document includes the following topics:

- [Security vulnerability fixes in InfoScale Operations Manager](#)

Security vulnerability fixes in InfoScale Operations Manager

The following are the 8 vulnerabilities (High - 3, Medium - 4, Low - 1) fixed in InfoScale Operations Manager 8.0.0.410 Security Patch. To receive the latest vulnerability fixes, you need to update their Management Servers to a minimum of version 8.0U4SP1 (8.0.0.410).

If you are using InfoScale version 7.2 or higher servers (newer), upgrading InfoScale Operations Manager Clients to version 8.0.0.410 is also possible. However, for servers running InfoScale version 7.1 or older, InfoScale Operations Manager Clients can be upgraded only to version 7.4.2.800.

For more information, visit [Veritas InfoScale Operations Manager \(VIOM\) Security Advisory](#)

Table 1-1

	Issuesname	Severity	Is Management Server impacted
1	Arbitrary Code Execution: The InfoScale Operations Manager web application does not validate the user supplied data and appends it to OS-commands and internal binaries used by the application. An attacker with root/administrator level privileges can use this vulnerability to read sensitive data stored on the servers, modify data or server configuration and delete data or application configuration.	High	Management Server and Clients

Table 1-1 *(continued)*

	Issuesname	Severity	Is Management Server impacted
2	SQL Injection: The InfoScale VIOM web application is vulnerable to SQL Injection in some of the areas of the application. This allows attackers to submit arbitrary SQL commands on the back-end database to create, read, update, delete any sensitive data stored in the database.	High	Management Server
3	Command Execution via Insecure File Upload: The InfoScale VIOM-XprtId web application allows an authenticated attacker to upload all types of files to the server. An attacker can execute the malicious file and gain complete control of back-end server.	High	Management Server and Clients
4	Cross-Site Request (CSRF) Forgery: The InfoScale VIOM web application is vulnerable to Cross-Site Request Forgery attacks. An attacker can coerce authenticated users into performing actions without their consent or knowledge of them performing that action.	Medium	Management Server
5	Cross-Site Scripting (XSS): The InfoScale VIOM web application is vulnerable to Cross-Site Scripting (XSS). An attacker can run malicious scripts in the context of the website in order to steal content stored in DOM and impersonate the user, coerce the user into carrying out unintended actions on the web application, or modify the content displayed to the user.	Medium	Management Server
6	CSV Excel Macro Injection: The InfoScale VIOM web application has a functionality that allows for users to export data in CSV format. This data is not sanitized and allows injection attacks against end-users who open the CSV files. By crafting special payloads, an attacker can run command-line programs via Microsoft Excel on a victim's machine in order to compromise their system.	Medium	Management Server
7	Arbitrary URL Redirection: The InfoScale VIOM web application redirects clients based on the navigation history without validation. While applications often need to redirect users between areas, this functionality can be used maliciously when implemented without adequate security controls. By crafting a special Webpage for victims, an attacker can trick a user into visiting a page that redirects them away from the safety of the application to the attacker's domain.	Low	Management Server

Table 1-1 (continued)

	Issuesname	Severity	Is Management Server impacted
8	Missing Authentication - Direct Request: The InfoScale VIOM web applications do not have sufficient authentication checks in place for accessing sensitive files and resources. This can allow an attacker to directly access the application resources without proper authentication and gain access to sensitive data	Medium	Management Server