

Security Advisories Relating to Veritas Products



NetBackup OpsCenter Server Reflected Cross-Site Scripting

October 1, 2015

SYM15-010

Revisions

20-April-2016 – Rereleased with Veritas information

Severity

CVSS2 Base Score	Impact	Exploitability	CVSS2 Vector
NetBackup OpsCenter Server Reflected XSS - High			
7.9	9.2	6.8	AV:N/AC:M/Au:S/C:C/I:C/A:N

Overview

Veritas NetBackup OpsCenter is an optional web based application that, if installed, is installed separately in a customer's environment for advanced monitoring, alerting, and reporting capabilities. Veritas NetBackup OpsCenter is susceptible to a reflected cross-site scripting (XSS) in the web console that could result in unauthorized access to the application with the privileges of the affected user's browser.

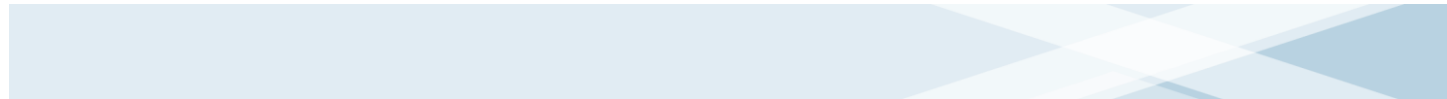
Affected Products

Product	Version	Solution(s)
Veritas NetBackup OpsCenter	7.7 and prior	Upgrade to Veritas NetBackup OpsCenter 7.7.1

Details

Veritas was notified of a reflected XSS in the optional Veritas NetBackup OpsCenter advanced monitoring, alerting, and reporting application console. XSS issues are the result of insufficient validation/sanitation of user input and server output. A successful exploitation of this issue is possible should a properly authenticated administrative user click on a maliciously-crafted link with a logged-in browser also being used to manage the OpsCenter console.

Cross-site scripting is a trust exploitation requiring enticing a previously authenticated user to click on a malicious URL. To be exposed to other than another authorized network user, an external attacker would need



to successfully entice an authorized, privileged Veritas OpsCenter console user to visit a malicious web site or click on a malicious HTML link in an email in any attempts to take advantage of this issue.

In a normal installation, the Veritas NetBackup OpsCenter should not be externally accessible from the network environment. Any attempt to exploit this issue would require network access either by an authorized network user or an external attacker able to gain unauthorized access to a logged-in authorized user's browser.

Veritas Response

Veritas engineers verified this issue and have resolved it in Veritas NetBackup OpsCenter 7.7.1. Customers should upgrade to this release to avoid potential incidents of this nature.

Veritas is not aware of exploitation of or adverse customer impact from these issues.

Update Information

NetBackup OpsCenter 7.7.1 is available through the following link for download and README information:

https://www.veritas.com/support/en_US/article.000094423

Best Practices

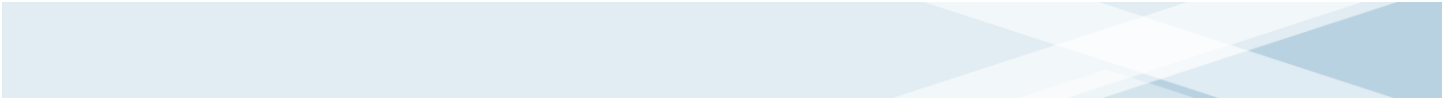
As part of normal best practices, Veritas strongly recommends that customers:

- 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 would like to thank Guy Dahan for reporting this issue and coordinating with us as we resolved it.

References



BID: Security Focus, <http://www.securityfocus.com>, has assigned a Bugtraq ID (BID) to this issue for inclusion in the Security Focus vulnerability database.

CVE: The issue is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

CVE	BID	Description
CVE-2015-6549	BID 76896	Veritas NetBackup OpsCenter Server Reflected XSS

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

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