Security Advisories Relating to Veritas Products

Backup Exec Multiple Issues

August 1, 2013 **SYM13-009**

Revisions

20-April-2016 – Rereleased with Veritas information

Severity

CVSS2 Base Score	Impact	Exploitability	CVSS2 Vector
Linux Agent Utility Heap Overflow – High			
7.9	10	5.5	AV:A/AC:M/Au:N/C:C/I:C/A:C
Management Console/beutility XSS - Medium			
3.7	4.9	4.1	AV:A/AC:L/Au:M/C:P/I:P/A:N
Backup Data Storage Files Weak Permissions - Medium			
4.3	6.4	3.1	AV:L/AC:L/Au:S/C:P/I:P/A:P
NDMP Information Disclosure - Low			
2.7	2.9	5.1	AV:A/AC:L/Au:S/C:P/I:N/A:N

Overview

Backup Exec is susceptible to security issues including a remote heap overflow in the utility program shipping with the Linux agent. Also potentially susceptible to cross-site scripting (XSS) issues in the management console, unauthorized access to backup data due to weak permissions and an information disclosure in the NDMP protocol. These issues could result in unauthorized OS version information disclosure, session hijacking/redirection or unauthorized access to sensitive information, crashing a Linux agent or potential elevation of privilege on a system hosting a Linux agent.

Affected Products

Product	Version	Build	Solution
Backup Exec	2012	1798	2012 SP2
Backup Exec	2010 R3	5204	2010 R3 SP3

Details

Veritas was notified of security issues with Backup Exec. The utility program shipping with the Linux agent used to back-up MAC/Unix/Linux clients is susceptible to a heap overflow that could potentially result in crashing the agent or possibly allow unauthorized privilege access to the host.

During a normal backup process, backup and restore data files are stored with weak ACLs allowing r/w access to everyone. This information could be useful to an authorized but non-privileged user able to access the stored data. The information could be used to leverage unauthorized access to or elevated privilege on network systems.

The NMDP protocol shipped with Backup Exec leaks host versioning information that could provide reconnaissance information to a malicious authorized user. The malicious user could potentially leverage this information for unauthorized access attempts against a network system.

The Backup Exec management console is susceptible to XSS issues in various pages used to generate custom reports, create Storage Devices and jobs. Beutility console is also susceptible to XSS issues when managing Backup Exec servers. A malicious user with authorized access to the management console or beutility could insert scripts that could be used to gather information from other authorized utility users potentially resulting in access to areas of the network or systems not normally authorized to them.

In a normal Backup Exec installation, neither agents nor servers should be accessible outside of the network environment. These restrictions reduce exposure to these issues from external sources. However, an external attacker able to successfully leverage network access or entice an authorized user to download a malicious code package could attempt to exploit some of these issues.

Veritas Response

Veritas engineers verified these issues and have released updates to address them. Customers should ensure they are on the latest release of Backup Exec 2012 or Backup Exec 2010 as indicated in the product matrix above.

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

Update Information

Updates are available through customers' normal support locations.

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 thanks Perran Hill, Shaun Jones, Edward Torkington, Daniele Costa, and Andy Davis with NCC Group for discovering, reporting these issues and coordinating with us as we addressed them

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-2013-4575	BID 61485	Linux Agent Utility Heap Overflow
CVE-2013-4676	BID 61486	Management Console/beutility Console XSS
CVE-2013-4677	BID 61487	Backup Data Storage Files Weak Permissions
CVE-2013-4678	BID 61488	NDMP Information Disclosure

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