

[Full-disclosure] ZDI-08-053: Symantec Veritas Storage Foundation Scheduler Service NULL Session Authentication Bypass Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-08/msg00326.html>

- *From:* zdi-disclosures@xxxxxxxx
 - *Date:* Thu, 14 Aug 2008 14:28:01 -0500
-

ZDI-08-053: Symantec Veritas Storage Foundation Scheduler Service NULL Session Authentication Bypass Vulnerability
<http://www.zerodayinitiative.com/advisories/ZDI-08-053>
August 14, 2008

— Affected Vendors:
Symantec

— Affected Products:
Symantec Veritas Storage Foundation

— Vulnerability Details:
This vulnerability allows an attacker to execute arbitrary code on vulnerable installations of Symantec Veritas Storage Foundation. User interaction is not required to exploit this vulnerability. Authentication is not required to exploit this vulnerability.

The specific flaw exists in the functionality exposed by the Storage Foundation for Windows Scheduler Service, VxSchedService.exe, which listens by default on TCP port 4888. The management console allows NULL NTLMSSP authentication thereby enabling a remote attacker to add, modify, or delete snapshots schedules and consequently run arbitrary code under the context of the SYSTEM user.

— Vendor Response:
Symantec has issued an update to correct this vulnerability. More details can be found at:

<http://www.symantec.com/avcenter/security/Content/2008.08.14a.html>

— Disclosure Timeline:
2008-06-26 – Vulnerability reported to vendor
2008-08-14 – Coordinated public release of advisory

— Credit:
This vulnerability was discovered by:

* Tenable Network Security

— About the Zero Day Initiative (ZDI):

Established by TippingPoint, The Zero Day Initiative (ZDI) represents a best-of-breed model for rewarding security researchers for responsibly disclosing discovered vulnerabilities.

Researchers interested in getting paid for their security research through the ZDI can find more information and sign-up at:

<http://www.zerodayinitiative.com>

The ZDI is unique in how the acquired vulnerability information is used. TippingPoint does not re-sell the vulnerability details or any exploit code. Instead, upon notifying the affected product vendor, TippingPoint provides its customers with zero day protection through its intrusion prevention technology. Explicit details regarding the specifics of the vulnerability are not exposed to any parties until an official vendor patch is publicly available. Furthermore, with the altruistic aim of helping to secure a broader user base, TippingPoint provides this vulnerability information confidentially to security vendors (including competitors) who have a vulnerability protection or mitigation product.

Our vulnerability disclosure policy is available online at:

http://www.zerodayinitiative.com/advisories/disclosure_policy/

CONFIDENTIALITY NOTICE: This e-mail message, including any attachments, is being sent by 3Com for the sole use of the intended recipient(s) and may contain confidential, proprietary and/or privileged information. Any unauthorized review, use, disclosure and/or distribution by any recipient is prohibited. If you are not the intended recipient, please delete and/or destroy all copies of this message regardless of form and any included attachments and notify 3Com immediately by contacting the sender via reply e-mail or forwarding to 3Com at postmaster@xxxxxxxx

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>