Security Advisory SWRX-2012-005

BreakingPoint Systems Storm CTM BugReport Information Disclosure Vulnerability

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: BreakingPoint Systems Storm CTM BugReport Information Disclosure Vulnerability
Advisory ID: SWRX-2012-005
Advisory URL: http://www.secureworks.com/research/advisories/SWRX-2012-005/
Date published: Wednesday, August 1, 2012
CVE: CVE-2012-2963
CVSS v2 base score: 5.0
Date of last update: Monday, July 23, 2012
Vendors contacted: BreakingPoint Systems
Release mode: Coordinated
Discovered by: Jeff Jarmoc, Dell SecureWorks

Summary

A vulnerability exists in BreakingPoint Systems Storm CTM due to insufficient controls placed on the administrative interface. The BreakingPoint Systems Storm CTM is used to test networks and data centers for resilience in the face of escalating application load and attack. Diagnostic requests supplied to the embedded web server are not properly checked for authentication and authorization. An unauthenticated remote attacker can leverage this issue to retrieve a diagnostic report of the system's configuration. This report includes sensitive information, including account names and email addresses of authorized users.

Affected products

BreakingPoint Systems Storm CTM V2.1.0.0 Build 71254:

http://www.breakingpointsystems.com/cyber-tomography-products/breakingpoint-storm-ctm/

Other versions may be affected, but have not been confirmed.

Vendor information, solutions and workarounds

The vendor has not released a fix that addresses this vulnerability at publication time.

As a workaround, use controls such as network segmentation and firewalls to limit access to the administrative interface of affected devices.

Details

A vulnerability exists in BreakingPoint Systems Storm CTM due to insufficient controls placed on the administrative interface. User-controllable requests supplied to the '/gwt/BugReport' script of the embedded web server are not properly checked for authorization. An unauthenticated remote attacker can leverage this issue to retrieve a diagnostic report of the system's configuration. This report, delivered as a .tgz archive, includes sensitive information such as system logs, test results, and detailed system configuration information as well as account names and email addresses of authorized users.

BreakingPoint appliances are not commonly exposed to the public Internet, which somewhat mitigates risks. The attacker must be able to directly communicate with the CTM's embedded web interface on port 80. Successfully exploiting this vulnerability could lead to disclosure of sensitive configuration information and account credentials.

This vulnerability was first reported to the vendor on April 5, 2011. Since April 8, 2011, Dell SecureWorks Counter Threat Unit™ (CTU) researchers have been working with members of the CERT® Coordination Center (CERT/CC), who have been coordinating disclosure with the vendor. Although originally stating that a fix would be available by fall 2011, the vendor delayed the release several times. The latest information is that the vulnerability will be addressed in version 3.0, scheduled for release by August 6, 2012.

CVSS severity (version 2.0)

Access Vector: Network
Access Complexity: Low
Authentication: Not required to exploit
Impact Type: Information disclosure
Confidentiality Impact: Partial
Integrity Impact: None
Availability Impact: None
CVSS v2 base score: 5.0
CVSS v2 impact subscore: 2.9
CVSS v2 exploitability subscore: 10.0
CVSS v2 vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Proof of concept

This issue can be duplicated by connecting a web browser to the following URL, replacing "www.example.com" with the name or IP address of the victim host:

```
http://www.example.com/gwt/BugReport
```

Revision history

1.0 2012-08-01: Initial advisory release

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit PGP key, which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer

This advisory may not be edited or modified in any way without the express written consent of Dell SecureWorks. Permission is hereby granted to link to this advisory via the Dell SecureWorks website or use in accordance with the fair use doctrine of U.S. copyright laws. See the Dell SecureWorks terms of use at http://www.secureworks.com/contact/terms_of_use/ for additional information.

The most recent version of this advisory may be found on the Dell SecureWorks website at www.secureworks.com. The contents of this advisory may change or be removed from the website without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. ANY USE OF THIS INFORMATION IS AT THE USER'S RISK. In no event shall Dell SecureWorks be liable for any damages whatsoever arising out of or in connection with the use or further publication or disclosure of this information.