Barracuda Networks Products
Multiple Directory Traversal Vulnerabilities

SecureWorks Security Advisory SWRX-2010-002

Advisory Information

Title: Barracuda Networks Products Multiple Directory Traversal Vulnerabilities
Advisory ID: SWRX-2010-002
Advisory URL: http://www.secureworks.com/ctu/advisories/SWRX-2010-002
Date published: Wednesday, September 29, 2010
CVSS v2 Base Score: 10 (High) (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Date of last update: Wednesday, September 29, 2010
Vendors contacted: Barracuda Networks
Release mode: Coordinated
Discovered by: Randy Janinda and corroborated by Sanjeev Sinha, SecureWorks

Summary

Multiple vulnerabilities exist in Barracuda Networks products due to improper validation of user-controlled input. User-controllable input supplied to the embedded web server is not properly sanitized for illegal path delimiting characters prior to being used to access files. A specially crafted HTTP request containing directory traversal sequences could allow remote attackers to conduct traversal attacks. The impact of successful exploitation depends upon the contents of the files that were retrieved.

Affected Products

Barracuda IM Firewall 3.4.01.004 and earlier
http://www.barracuda.com/ns/products/im_overview.php

Barracuda Link Balancer 2.1.1.010 and earlier
http://www.barracuda.com/ns/products/link_overview.php

Barracuda Load Balancer 3.3.1.005 and earlier
http://www.barracuda.com/ns/products/balancer_overview.php

Barracuda Message Archiver 2.2.1.005 and earlier
http://www.barracuda.com/ns/products/archiver-overview.php

Barracuda Spam & Virus Firewall 4.1.2.006 and earlier
http://www.barracudanetworks.com/ns/products/spam_overview.php

Barracuda SSL VPN 1.7.2.004 and earlier

http://www.barracudanetworks.com/ns/products/sslvpn_overview.php

Barracuda Web Application Firewall 7.4.0.022 and earlier
http://www.barracuda.com/ns/products/web-site-firewall-overview.php

Barracuda Web Filter 4.3.0.013 and earlier
http://www.barracudanetworks.com/ns/products/web-filter-overview.php

Vendor Information, Solutions and Workarounds

The vendor has released Security Definition update v2.0.4 that addresses these vulnerabilities. Barracuda Networks products should automatically download and apply this Security Definition update by default. Users of affected Barracuda Networks products should verify that Security Definition v2.0.4 has been successfully applied.

Details

Directory traversal vulnerabilities are present in eight different Barracuda Networks products: Barracuda IM Firewall, Barracuda Link Balancer, Barracuda Load Balancer, Barracuda Message Archiver, Barracuda Spam & Virus Firewall, Barracuda SSL VPN, Barracuda Web Application Firewall and Barracuda Web Filter. By sending a specially crafted HTTP request containing directory traversal sequences, a remote attacker may retrieve arbitrary files within the context of the product's embedded web server.

Successful exploitation of these vulnerabilities could lead to full remote administrative access to the vulnerable products. After obtaining administrative access, an attacker may be able to create, modify, or delete user accounts, read stored messages, purge system logs, and access sensitive and/or confidential information.

SecureWorks Risk Scoring

Likelihood *(scale of 1-5, with 5 being high)*: 4 – These devices are designed to be on the perimeter of a network and to offer remote network access. Access to the vulnerable web interface may have been restricted via network access controls per security best practices, reducing the likelihood of exploitation.

Impact *(scale of 1-5, with 5 being high)*: 5 – Successfully exploiting this vulnerability could lead to complete compromise of the vulnerable device.

CVSS Severity (version 2.0)

Access Vector: Network exploitable
Access Complexity: Low
Authentication: Not required to exploit
Confidentiality Impact: Complete
Integrity Impact: Complete
Availability Impact: Complete
Impact Subscore: 10
Exploitability Subscore: 10
CVSS v2 Base Score: 10 (High) (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Proof of Concept

The two URLs below will reproduce the issue. Note that the device in question must be configured to run the embedded web server. In the examples below, the embedded web server is running on TCP port 8000. The use of cleartext HTTP allows eavesdropping on the requests and responses.

```
http://<ip_address>:8000/cgi-
mod/view_help.cgi?locale=/..//../..//../..//../..//../..//etc/passwd%00
```

```
http://<ip_address>:8000/cgi-
mod/view_help.cgi?locale=/..//../..//../..//../..//../..//home/product/code/firmware/cu
rrent/apache/logs/access_log%00
```

The access_log retrieved in the second example above may contain the device's administrative password, which may be stored in cleartext.

Revision History

1.0 2010-09-29 – Initial advisory release

1.1 2010-09-29 – Updated to include all eight impacted products. Updated to include more information on affected firmware revisions.

PGP Keys

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

About the SecureWorks Counter Threat Unit℠

Our expert team of threat researchers, also known as the SecureWorks Counter Threat Unit℠, identifies and analyzes emerging threats and develops countermeasures, correlations and SOC processes to protect clients' critical information assets. The CTU frequently serves as an expert resource for the media, publishes technical analyses for the security community and speaks about emerging threats at security conferences. Leveraging our security technologies and a network of industry contacts, the CTU tracks leading hackers and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables the CTU to identify threats as they emerge and develop countermeasures that protect our clients before damage occurs.

About SecureWorks

SecureWorks is a leading provider of world-class information security services with over 2,800 clients worldwide. Organizations of all sizes, including more than ten percent of the Fortune 500, rely on SecureWorks to protect their assets, support compliance and reduce costs. The combination of deep security knowledge and expertise, purpose-built security technology and processes and excellent client service makes SecureWorks the premier provider of information security services. Positioned in the Leader's Quadrant of Gartner's Magic Quadrant for MSSPs, SecureWorks has been recognized by SC

Magazine's readers with the “Best Managed Security Service” award for 2006, 2007, 2008 & 2009 and has been named to the Inc. 500, Inc. 5000 and Deloitte lists of fastest-growing companies.

Disclaimer