

TSRT-06-07: eIQnetworks Enterprise Security Analyzer Monitoring Agent Buffer Overflow Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-08/msg00161.html>

- *From:* TSRT@xxxxxxxxx
 - *Date:* Tue, 8 Aug 2006 11:00:38 -0700
-

TSRT-06-07: eIQnetworks Enterprise Security Analyzer Monitoring Agent Buffer Overflow Vulnerabilities

<http://www.tippingpoint.com/security/advisories/TSRT-06-07.html>

August 8, 2006

-- CVE ID:
CVE-2006-3838

-- Affected Vendor:
eIQnetworks

-- Affected Products:
Enterprise Security Analyzer

-- TippingPoint(TM) IPS Customer Protection:
TippingPoint IPS customers have been protected against this vulnerability since July 31, 2006 by Digital Vaccine protection filter ID 4386. For further product information on the TippingPoint IPS:

<http://www.tippingpoint.com>

-- Vulnerability Details:
These vulnerabilities allow remote attackers to execute arbitrary code on vulnerable installations of eIQnetworks Enterprise Security Analyzer. Authentication is not required to exploit these vulnerabilities.

The first flaw specifically exists within the routines responsible for handling user-supplied data on TCP port 9999 within Monitoring.exe. Upon connecting to this port the user is immediately prompted for a password. A custom string comparison loop is used to validate the supplied password against the hard-coded value "eiq2esa?", where the question mark represents any alpha-numeric character. Issuing the command "HELP" reveals a number of documented commands:

Usage:

QUERYMONITOR: to fetch events for a particular monitor

QUERYMONITOR&<user>&<monid>&timer

QUERYEVENTCOUNT or QEC: to get latest event counts

RESETEVENTCOUNT or REC: to reset event counts

REC&[ALL] or REC&dev1,dev2,

STATUS: Display the running status of all the threads

TRACE: TRACE&ip or hostname&. TRACE&OFF& will turn off the trace

FLUSH: reset monitors as though the hour has changed

ALRT-OFF and ALRT-ON: toggle the life of alerts-thread.

RECV-OFF and RECV-ON: toggle the life of event-collection thread.

EM-OFF and EM-ON toggle event manager

DMON-OFF and DMON-ON toggle device event monitoring

HMON-OFF and HMON-ON toggle host event monitoring

NFMON-OFF and NFMON-ON toggle netflow event monitoring

HPMON-OFF and HPMON-ON toggle host perf monitoring

X or EXIT: to close the session

Supplying a long string to the TRACE command results in an overflow of the global variable at 0x004B1788. A neighboring global variable, 116 bytes after the overflowed variable, contains a file output stream pointer that is written to every 30 seconds by a garbage collection thread. The log message can be influenced and therefore this is a valid exploit vector, albeit complicated. A trivial exploit vector exists within the parsing of the actual command at the following equivalent API call:

```
sscanf(socket_data, "%[^&]&%[^&]&", 60_byte_stack_var, global_var);
```

Because no explicit check is made for the exact command "TRACE", an attacker can abuse this call to sscanf by passing a long suffix to the TRACE command that is free of the field terminating character, '&'. This vector is trivial to exploit.

The second flaw specifically exists within the routines responsible for handling user-supplied data on TCP port 10626 within Monitoring.exe. The service will accept up to approximately 16K of data from unauthenticated clients which is later parsed, in a similar fashion to above, in search of the delimiting character '&'. Various trivial vectors of exploitation exist, for example, through the QUERYMONITOR command.

— Vendor Response:

eIQnetworks has issued an update to correct this vulnerability. More details can be found at:

http://www.eiqnetworks.com/products/enterprisesecurity/EnterpriseSecurityAnalyzer/ESA_2.5.0_Release_Notes.pdf

— Disclosure Timeline:

TSRT-06-07: eIQnetworks Enterprise Security Analyzer Monitoring Agent Buffer Overflow Vulnerabilities

2006.05.10 – Vulnerability reported to vendor

2006.07.31 – Digital Vaccine released to TippingPoint customers

2006.08.08 – Coordinated public release of advisory

— Credit:

This vulnerability was discovered by Pedram Amini, TippingPoint Security Research Team.

— About the TippingPoint Security Research Team (TSRT):

The TippingPoint Security Research Team (TSRT) consists of industry recognized security researchers that apply their cutting-edge engineering, reverse engineering and analysis talents in our daily operations. More information about the team is available at:

<http://www.tippingpoint.com/security>

The by-product of these efforts fuels the creation of vulnerability filters that are automatically delivered to our customers' intrusion prevention systems through the Digital Vaccine(R) service.