

# [UNIX] Multiple Vulnerabilities in Monit

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-04/0029.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 04/11/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 11 Apr 2004 15:09:57 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Multiple Vulnerabilities in Monit

---

## SUMMARY

<<http://www.tildeslash.com/monit/>> Monit is "a utility for managing and monitoring, processes, files, directories and devices on a UNIX system. Monit conducts automatic maintenance and repair and can execute meaningful causal actions in error situations". Several vulnerabilities allow a remote attacker with access to Monit's WBA via HTTP or HTTPS clients to potentially gain the privileges of the root user.

## DETAILS

### Vulnerable Systems:

- \* Stable: Monit 4.2 and prior
- \* Beta: Monit 4.3 Beta 2 and prior

### Immune Systems:

- \* Stable: Monit 4.2.1
- \* Beta: Monit 4.3 Beta 3

Three vulnerabilities were found in Monit during a simple code review. All of the vulnerabilities are in Monit's HTTP/HTTPS administration interfaces, and as such can only be exploited if the interface is enabled and accessible. Two of the vulnerabilities lie in the Basic authentication

## Securiteam: [UNIX] Multiple Vulnerabilities in Monit

code, while one vulnerability lies in the processing of POST requests.

### \* Basic Authentication Out-of-Bounds Read (Denial of Service)

When faced with a Basic authentication request without a password, Monit will decrement a pointer returned by a strchr() call without appropriate NULL pointer checking. The error results in a segmentation fault during a strcpy() call. This request can be generated with a simple web browser. This vulnerability does not allow users to gain privileges on the server. For instance. Specifically, if the base64-decoded credentials string does not contain a colon, the vulnerability can be exploited.

### \* Basic Authentication Buffer Overflow (Remote Root)

When faced with a Basic authentication request with an overly long user name (> 256 characters), vulnerable versions of Monit will overrun a stack-based buffer. This potentially allows a remote attacker to gain root privileges.

### \* POST Input Off-By-One (Exploitability Varies)

When faced with a POST submission that is exactly 1,024 bytes, Monit suffers from an off-by-one overflow. The ability to exploit this vulnerability depends on the version of gcc used to compile the application. Some compilers will allow this overflow to modify the frame pointer, potentially controlling stack frames.

### \* Integer Overflow in POST Input Handler (UPDATE to the vulnerability discovered by S-Quadra)

S-Quadra discovered that a large HTTP POST would cause an xmalloc() call within the WBA to fail. This issue was fixed in 4.2.1 as a denial of service. In fact, this code also contained an exploitable integer overflow. By specifying a Content-Length header of -1, a zero-byte heap allocation is performed. An attacker can then input an arbitrary amount of data, overwriting significant portions of the heap. Matthew Murphy's research suggests that this issue could also be exploited.

### Vendor Status:

April 3, 2004:

- \* First two vulnerabilities discovered
- \* Monit team notified via e-mail (monitgroup@tildeslash.com)

April 4, 2004:

- \* Response from Jan Henrik-Haukeland (hauk@tildeslash.com)
- \* Patch for first two reports committed to CVS
- \* Third vulnerability discovered
- \* Monit team notified via e-mail (monitgroup@tildeslash.com)

April 5, 2004:

- \* Response from Jan Henrik-Haukeland (hauk@tildeslash.com)
- \* Patch for third issue committed to CVS
- \* Monit team releases security advisory
- \* Monit 4.2.1 released
- \* Monit 4.3 Beta 3 released
- \* Public disclosure

## Securiteam: [UNIX] Multiple Vulnerabilities in Monit

The Monit team deserves praise on a very speedy response to this vulnerability. Particularly noteworthy is that the vendor was notified shortly before midnight on April 4, 2004. The patch for each of these issues was committed to CVS within 18 hours of the initial report. Thanks to Jan Henrik-Haukeland for a fast response to this issue.

### Workaround

For those who cannot immediately upgrade packages, it is recommended that the Monit HTTP interface be disabled. If access to this interface is necessary, limit it to the Local Area Network with appropriate firewall rules. Upgrading as listed below is recommended if possible. For those users of Monit who have deployed vendor-provided packages, it is recommended to wait for updated vendor binaries.

### Solution

\* Monit 4.2 Stable: The vendor has released Monit 4.2.1, which contains these fixes. It can be downloaded at:

<<http://www.tildeslash.com/monit/dist/monit-4.2.1.tar.gz>>

<http://www.tildeslash.com/monit/dist/monit-4.2.1.tar.gz>

MD5 Checksum:

<<http://www.tildeslash.com/monit/dist/monit-4.2.1.tar.gz.md5>>

<http://www.tildeslash.com/monit/dist/monit-4.2.1.tar.gz.md5>

\* Monit 4.3 Beta: The vendor has released Monit 4.3 Beta 3, which contains these fixes. It can be downloaded at:

<<http://www.tildeslash.com/monit/beta/monit-4.3-beta3.tar.gz>>

<http://www.tildeslash.com/monit/beta/monit-4.3-beta3.tar.gz>

MD5 Checksum:

<<http://www.tildeslash.com/monit/beta/monit-4.3-beta3.tar.gz.md5>>

<http://www.tildeslash.com/monit/beta/monit-4.3-beta3.tar.gz.md5>

Vendor's official advisory can be found at:

<[http://www.tildeslash.com/monit/secadv\\_20040305.txt](http://www.tildeslash.com/monit/secadv_20040305.txt)>

[http://www.tildeslash.com/monit/secadv\\_20040305.txt](http://www.tildeslash.com/monit/secadv_20040305.txt)

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:mattmurphy@kc.rr.com>>  
Matthew Murphy.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

## Securiteam: [UNIX] Multiple Vulnerabilities in Monit

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.