Security Announcements

June 19th, 2019

Multiple vulnerabilities were found in 3rd party software running on the Men & Mice appliances.

- A vulnerability, CVE-2019-6471 was found in 3rd party software running on our DNS/DHCP appliance.

  A race condition which may occur when discarding malformed packets can result in BIND exiting due to a REQUIRE assertion failure in dispatch.c.

  An attacker who can cause a resolver to perform queries which will be answered by a server which responds with deliberately malformed answers can cause named to exit, denying service to clients.

  For more information, see https://kb.isc.org/docs/cve-2019-6471.

- Multiple vulnerabilities, CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479, were found in the Linux kernel that is used on the Men & Mice appliances
  In some cases, the vulnerability could allow an attacker to trigger a kernel panic in the system.

We recommend that all Men & Mice Appliances are upgraded to the latest version, 9.2.4.

Updates to the other supported branches, 8.3 and 9.1 will follow.

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

April 25th, 2019

A vulnerability, CVE-2018-5743 was found in 3rd party software running on our DNS/DHCP appliance.

A defect in BIND's handling the number of TCP clients could allow an attacker to grow the number of simultaneous connections beyond the limit, which would result in unexpected and unreliable behavior.

For more information, see https://kb.isc.org/docs/cve-2018-5743.

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to the latest version, either 9.1.11 or 9.2.2.

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

September 20th, 2018

This is an critical operational announcement from Men & Mice.

An issue was found in 3rd party software running on our Caching appliances. A critical issue was found in an internal tool that is used to update trust anchors for the
Unbound DNS server. Consequently, the DNS server on the Caching Appliance was upgraded to version 1.6.5.

A KSK key rollover is scheduled for the root zone on the 11th of October 2018 and before, Unbound must be able to update the trust anchors automatically. That has been fixed in version 1.6.5 of Unbound and in version 9.1.4 of the Men & Mice Suite.

We recommend that all Men & Mice Appliances are upgraded to the latest version, which is 9.1.4.
The appliances on the 8.3 and 8.1 versions will be available on the 26th of September 2018.

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

June 30th, 2017

The following vulnerabilities were found in 3rd party software running on our DNS/DHCP appliance:

- CVE-2017-3142: An error in TSIG authentication can permit unauthorized zone transfers. See for https://kb.isc.org/article/AA-01504 more details.
- CVE-2017-3143: An error in TSIG authentication can permit unauthorized dynamic updates. See for https://kb.isc.org/article/AA-01503 m ore details.

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to one of the following versions:

- **LTS versions 7.1.14 or 8.1.4**
- **8.2.1**

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

April 12th, 2017

Multiple vulnerabilities were found in 3rd party software running on our DNS/DHCP appliance:

- CVE-2017-3136: An error handling synthesized records could cause an assertion failure when using DNS64 with "break-dnssec yes;". See for https://kb.isc.org/article/AA-01465 more details.
- CVE-2017-3137: A response packet can cause a resolver to terminate when processing an answer containing a CNAME or DNAME. See https://kb.isc.org/article/AA-01466 for more details.
- CVE-2017-3138: named exits with a REQUIRE assertion failure if it receives a null command string on its control channel. See https://kb.i sc.org/article/AA-01471 for more details.

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to either 7.1.13 or 8.1.2. Both versions are LTS versions.

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

January 12th 2017.

Multiple vulnerabilities were found in 3rd party software running on our DNS/DHCP appliance:

- CVE-2016-9131: A malformed response to an ANY query can cause an assertion failure during recursion. See https://kb.isc.org/article/A A-01439 for more details.
- CVE-2016-9147: An error handling a query response containing inconsistent DNSSEC information could cause an assertion failure. See https://kb.isc.org/article/AA-01440 for more details.
- CVE-2016-9444: An unusually-formed DS record response could cause an assertion failure. See https://kb.isc.org/article/AA-01441 for more details.

- CVE-2016-9778: An error handling certain queries using the nxdomain-redirect feature could cause a REQUIRE assertion failure in db.c. See https://kb.isc.org/article/AA-01442 for more details.

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to the latest version, which is 7.3.2.

The appliances on the 7.1 LTS version have also been updated. The latest version in 7.1 is 7.1.12

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

November 1st, 2016

A vulnerability, CVE-2016-8864 was found in 3rd party software running on our DNS/DHCP appliance.

A defect in BIND's handling of responses containing a DNAME answer can cause a resolver to exit
after encountering an assertion failure in db.c or resolver.c

For more information, see https://kb.isc.org/article/AA-01434.

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to the latest version, which is 7.2.7.

The appliances on the 7.1 version have also been updated. The latest version in 7.1 is 7.1.11

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

September 28th, 2016

A vulnerability, CVE-2016-2776 was found in 3rd party software running on our DNS/DHCP appliance.

A defect in BIND can cause the named process to exit with an assertion failure when constructing a response to a specific query.

For more information, see https://kb.isc.org/article/AA-01419.

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to the latest version, which is 7.2.4.

The appliances on the 7.1 version have also been updated. The latest version in 7.1 is 7.1.9

The appliances can be easily upgraded using the Automatic Updates feature of the Men & Mice Suite.
For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

March 10th, 2016

Two vulnerabilities, CVE-2016-1285 and CVE-2016-1286, were found in 3rd party software running on our DNS/DHCP appliances.

For more information, see https://kb.isc.org/article/AA-01352 and https://kb.isc.org/article/AA-01353. These vulnerabilities have been fixed in the latest version of the Men & Mice Suite.

Additionally, a vulnerability, CVE-2016-2774, was found in the ISC DHCP server software running on the DNS/DHCP appliance.

By exploiting this vulnerability, an attacker could interfere with the DHCP server operation. A patch is expected later in March, but until then a workaround is that server operators should restrict the hosts allowed to make connections to DHCP server inter-process communication channels to trusted hosts, blocking connections to the OMAPI control port and the failover communications ports from all other hosts.

For more information, see https://kb.isc.org/article/AA-01354

We recommend that all Men & Mice Appliances are upgraded to the latest version, which is 7.1.4.

The appliances on the 6.8 version have also been updated. The latest version in 6.8 is 6.8.11.

The appliances can be easily upgraded using the Automatic Update feature of the Men & Mice Suite.

For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below

https://docs.menandmice.com/display/MM/Contacting+Support

See the Security Announcements Archive for details on previous security announcements

https://docs.menandmice.com/display/MM/Security+Announcements

---

March 3rd, 2016

A vulnerability was found in 3rd party software running on our DNS/DHCP and Caching appliances.

A critical bug was found in the glibc linux library. A remote attacker could crash or, potentially, execute code running the library on Linux.

There are no workarounds other than upgrading the appliance.

We recommend that all Men & Mice Appliances are upgraded to the latest version, which is 7.1.3.

The appliances on the 6.8 version have also been updated. The latest version in 6.8 is 6.8.10.

The appliances can be easily upgraded using the Automatic Update feature of the Men & Mice Suite.

For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below

https://docs.menandmice.com/display/MM/Contacting+Support

See the Security Announcements Archive for details on previous security announcements

https://docs.menandmice.com/display/MM/Security+Announcements

---

February 19th, 2015

A vulnerability was found in 3rd party software running on our DNS/DHCP appliance.

BIND, the DNS server running on the DNS/DHCP appliance has been found to be vulnerable where it can crash under certain conditions. This vulnerability has been registered as CVE-2015-1349.

When configured to perform DNSSEC validation, the DNS server can crash when encountering a rare set of conditions in the managed trust anchors.

There is no workaround other than upgrading the appliance.

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to the latest version, which is 6.7.6.

The appliances can be easily upgraded using the Automatic Update feature of the Men & Mice Suite.

For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

December 15th, 2014

A vulnerability was found in 3rd party software running on our DNS/DHCP appliance.

Due to the "POODLE" vulnerability, the SSLv3 protocol is now disabled on the Men & Mice appliances

We recommend that all Men & Mice DNS/DHCP Appliances are upgraded to the latest version, which is 6.7.4.

The appliances can be easily upgraded using the Automatic Update feature of the Men & Mice Suite.

For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support

December 8th, 2014

A vulnerability was found in 3rd party software running on our DNS/DHCP appliance and Caching appliance.

A vulnerability was found and patched in Unbound (CVE-2014-8602). Two vulnerabilities were found and patched in BIND (CVE-2014-8500 and CVE-2014-8680)

We recommend that all Men & Mice DNS/DHCP Appliances and Caching appliances are upgraded to the latest version, which is 6.7.3.

The appliances can be easily upgraded using the Automatic Update feature of the Men & Mice Suite.

For details on how to update the Men & Mice Suite, see

https://docs.menandmice.com/display/MM/Updating+the+Men+and+Mice+Suite

For more information regarding the upgrade, contact Men & Mice Support using the link below
https://docs.menandmice.com/display/MM/Contacting+Support