Security Advisory – Local Privilege Escalation Vulnerability in otris "Update Manager"

Title:	Local Privilege Escalation Vulnerability in otris "Update Manager"
Last Modification:	31.01.2022
Version:	1.0
Classification:	Public
Status:	Final
Vendor:	otris software AG
Product:	Software component “Update Manager”
Affected Version:	1.2.1.0 (Confirmed)
Other affected Versions:	Unknown
Fixed in Version:	N/A
Credits:	Shadi Habbal, TÜV Rheinland i-sec GmbH
CVSSv3 Score:	8.8 (High)
CVSSv3 Vector:	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CVE-ID:	CVE-2021-40376
Summary:	“Update Manager”, a software component used by multiple otris applications, e.g. *otris Privacy*, allows local users to escalate their privileges on Windows systems to SYSTEM, by exploiting a vulnerability in the aforementioned software, which runs as a highly privileged Windows service.

Description:

“Update Manager” is a software component used by multiple otris applications, e.g. *otris Privacy*, to manage updates of their software on Windows systems. The software component is installed as a Windows service, and is executed with the rights of SYSTEM. The nature of the software requires elevated privileges in order to install updates and/or add/remove programs.

The affected software component accepts local connections via *.NET named pipes* and remote connections over HTTP port *9000* via *WsHTTPBinding*.

While examining the way “Update Manager” handles local connections over *.NET named pipes* the security researcher discovered a vulnerability, which would allow a local attacker (or an attacker logged on remotely to the target machine) to escalate his privileges on the affected Windows machine to those of SYSTEM.

The vulnerability can be exploited by connecting to the vulnerable component “Update Manager” via *.NET named pipes* on the same target machine and issuing direct calls to available functions on the exposed interface, which are processed by the vulnerable component without any form of prior authentication.

In order to achieve local privilege escalation, different approaches exist. In hardened corporate environments, where executing MSI files is not allowed due to enforced policy restrictions, an attacker can opt for overwriting the executables of any privileged Windows services or privileged *Scheduled Task* on paths not protected by Windows File Protection (WFP)[1]. For instance, attackers can opt to overwrite an executable located under (incl. sub folders) “*C:\Program Files*” or “*C:\Program Files (x86)*”. These paths are not protected by WFP and would facilitate the attack.

When exploiting the vulnerability by opting to overwriting an executable of a privileged Windows service or scheduled task, attackers need to overcome an obstacle. The “*saveUpdateFiles*” function in the “*UpdateProcessorClient*” interface extracts attacker-controllable ZIP files to attacker-controllable paths, however, the “*ProductId*” (an attacker-controllable GUID) in the “*ProductDefinition*” is padded to the path where the ZIP file’s content are extracted. For example, an attacker who wish to overwrite the file “*C:\Target\Executable.exe*”, would find that the overwritten path becomes “*C:\Target\01234567-1234-5678-1234-0123456789123\Executable.exe*”, (where “*01234567-1234-5678-1234-0123456789123*” is an exemplary GUID), and that renders the attack useless. However, attackers can facilitate the ZIP Slip Vulnerability[2] and prepare a malicious ZIP file with ZIP entries called “..”, which are used as part of the filename when preparing the path. When the extraction path is prepared, the overwritten path becomes “*C:\Target\01234567-1234-5678-1234-0123456789123\..\Executable.exe*”.
This was tested successfully against the “*extractZipFile*” function responsible for extracting ZIP files.

The vulnerability was found and exploited against production systems with active EDR and anti-virus software; during a penetration test conducted by the security researcher.

Exploitation of this vulnerability remotely over *WsHTTPBinding* is not excluded and should be further investigated.

Disclosure Timeline:

20.08.2021	Initial notification per email (<info@otris.de>) to locate the suitable contact person
27.08.2021	No response. Forward of initial notification to (<support@otris.de>)

[1] https://support.microsoft.com/en-us/topic/description-of-the-windows-file-protection-feature-db28f515-6512-63d1-6178-982ed2022ffb
[2] https://snyk.io/research/zip-slip-vulnerability

27.08.2021	Contact data of responsible person are provided
01.09.2021	This document in v1.0 is shared with the contact person
13.09.2021	otris Software AG suggest a fix per email. Asks for expert review. No binaries provided
15.09.2021	Based on pure provided information, expert concludes that the suggested solution is not sufficient
06.10.2021	otris Software AG shares further information and mentions removal of vulnerable component in newer versions of affected software. With the suggested fix, the vulnerability will be considered by otris Software AG as fixed
01.12.2021	90 days after responsible disclosure are over. TÜV Rheinland i-sec GmbH decides to grant an additional 60 days considering the vacation/holidays season to enable end-users to patch their systems
31.01.2022	Preparation for publish.