

master

...

Vulnerability-Disclosures / 2022 / MNDT-2022-0023 / MNDT-2022-0023.md

Aaron Carreras Add BigFix CVE-2021-27765, CVE-2021-27766, and CVE-2021-27767 for Ronnie ...

History

0 contributors

38 lines (27 sloc) | 1.72 KB

...

MNDT-2022-0023

Description

HCL BigFix Server API for Windows contains a local privilege escalation vulnerability prior to version 10.0.6/9.5.19.

Impact

High - Exploiting the vulnerability will give a local unprivileged attacker SYSTEM level privileges.

Exploitability

Medium - Any authenticated local user can exploit the vulnerability and an exploit is trivial to produce.

CVE Reference

CVE-2021-27765

Common Weakness Enumeration

CWE-379: Creation of Temporary File in Directory with Insecure Permissions

Common Vulnerability Scoring System

Base Score: 7.8 - Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Technical Details

The installation of the agent uses the Windows Installer framework and an MSI file is cached in c:\windows\installer. An unprivileged user can trigger a repair operation, either by using the Windows Installer API or by running "msiexec.exe /fa c:\windows\installer\[XXXXX].msi".

Running a repair operation will trigger a number of file operations in the %TEMP% folder of the user triggering the repair. Some of these operations will be performed from a SYSTEM context (started via the Windows Installer service), including the execution of temporary files.

Resolution

The issue was fixed in version 10.0.6/9.5.19. Update to this version to address the vulnerability.

Discovery Credits

- Ronnie Salomonsen, Mandiant

Disclosure Timeline

- 28-Sep-2021 - Issue reported to HCL
- 19-Dec-2021 - Issue confirmed by HCL and a fix scheduled for April 21, 2022.
- 21-Apr-2022 - Patched version released by HCL

References

- [HCL Security Bulletin](#)
- [Mitre CVE-2021-27765](#)