1E Security Advisory-1E Client for Windows: CVE-2020-16268, CVE-2020-27643, CVE-2020-27644, CVE-2020-27645

Vulnerability Summary

CVE IDs:	Impact of Vulnerabilities:	Severity Ratings:	CVSS v3.1 Base/Temporal Scores:
CVE-2020-16268	Execution with Unnecessary Privileges	Medium	6.0 / 5.4
CVE-2020-27643	Windows Hard Link	Medium	5.4 / 4.9
CVE-2020-27644	Uncontrolled Search Path Element	Medium	6.8 / 6.1
CVE-2020-27645	Unquoted Search Path or Element	Medium	6.8 / 6.1
Highest Severity Rating	Medium		
Recommendations	Install the latest 1E Client Hotfix • Cumulative update Q21140 (or later) for 1E Client 5.0.0.745 Update to latest 1E Client release • Update 1E Client 5.1.0.922		
Security Bulletin Replacement	None		
Affected Software	1E Client for Windows: • 5.0.x • 4.1.x		
Location of updated software	1E Client Product Downloads		

Vulnerability Description

This Security Bulletin covers four vulnerabilities in 1E Client. The fixes for these vulnerabilities can be found in the following releases.

	1E Client 4.1.0.267	1E Client 5.0.0.745
CVE-2020-16268	Vulnerable under specific circumstances, see notes below. Fixed in 5.1.0.922 and higher.	Vulnerable under specific circumstances, see notes below. Fixed in 5.1.0.922 and higher.
CVE-2020-27643	Vulnerable. Mitigation available. This vulnerability can be mitigated by changing the permission of the C:\ProgramData\1E\Client directory so that a standard user does not have the ability to create and modify files. Fixed in 5.1.0.922 and higher.	Vulnerable. Mitigation available. This vulnerability can be mitigated by changing the permission of the C:\ProgramData\1E\Client directory so that a standard user does not have the ability to create and modify files. Fixed in 5.1.0.922 and higher.
CVE-2020-27644	Not vulnerable	Fixed This vulnerability has been fixed in Q21139 Hotfix that was first released as part of Cumulative update Q21140 for 1E Client 5.0.0.745 on 1st September 2020
CVE-2020-27645	Not vulnerable	Fixed This vulnerability has been fixed in Q21135 Hotfix that was first released as part of Cumulative update Q21140 for 1E Client 5.0.0.745 on 1st September 2020

CVE-2020-16268 - Execution with Unnecessary Privileges

Description:

The MSI installer in 1E Client 4.1.0.267 and 5.0.0.745 allows remote authenticated users and local users to gain elevated privileges via the repair option. This applies to installations that have a TRANSFORM (MST) with the option to disable the installation of the Nomad module. An attacker may craft a .reg file in a specific location that will be able to write to any registry key as an elevated user.

CVSS v3.1 Vector AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:L/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X

https://nvd.nist.gov/vuln/detail/CVE-2020-16268
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16268

CVE-2020-27643 - Windows Hard Link

Description:

The %PROGRAMDATA%\1E\Client directory in 1E Client 5.0.0.745 and 4.1.0.267 allows remote authenticated users and local users to create and modify files in protected directories (where they would not normally have access to create or modify files) via the creation of a junction point to a system directory. This leads to partial privilege escalation. This vulnerability can be mitigated by changing the permission of the ProgramData\1E\Client directory so that a standard user does not have the ability to create and modify files.

CVSS v3.1 Vector AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C

https://nvd.nist.gov/vuln/detail/CVE-2020-27643
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27643

CVE-2020-27644 - Uncontrolled Search Path Element

Description:

The Inventory module of the 1E Client 5.0.0.745 doesn't handle an unquoted path when executing %PROGRAMFILES%\1E\Client\Tachyon.Performance.Metrics.exe. This may allow remote
authenticated users and local users to gain elevated privileges by placing a malicious file called cryptbase.dll to the C:\Windows\Temp\.

CVSS v3.1 Vector AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

https://nvd.nist.gov/vuln/detail/CVE-2020-27644
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27644

CVE-2020-27645 - Unquoted Search Path or Element

Description:

The Inventory module of the 1E Client 5.0.0.745 doesn't handle an unquoted path when executing %PROGRAMFILES%\1E\Client\Tachyon.Performance.Metrics.exe. This may allow remote
authenticated users and local users to gain elevated privileges.

CVSS v3.1 Vector AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

https://nvd.nist.gov/vuln/detail/CVE-2020-27645
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27645

Remediation
To remediate these issues:

- 1E Client 4.1.0.267 - Upgrade to 1E Client 5.1.0.922 Sep 25, 2020 Update.
- 1E Client 5.0.0.745 - Upgrade to 1E Client 5.1.0.922 Sep 25, 2020 Update or apply Cumulative Hotfix Q21140 for 1E Client 5.0.0.745 1st September 2020.

Go to the 1E Client Product Downloads site, and download the applicable product update/hotfix file:

Product	Version	Type	Release Date
1E Client	5.1 Update	Update	Sep 25, 2020
1E Client	Cumulative Hotfix Q21140 (or later) for 1E Client 5.0.0.745	Hotfix	Sept 1, 2020

Acknowledgments
CVE-2020-16268 - 1E thanks **Lockheed Martin Red Team** for responsibly disclosing this flaw.
CVE-2020-27643 - 1E thanks **Lockheed Martin Red Team** for responsibly disclosing this flaw.
CVE-2020-27644 - 1E thanks **Lockheed Martin Red Team** for responsibly disclosing this flaw.
CVE-2020-27645 - 1E thanks **Lockheed Martin Red Team** for responsibly disclosing this flaw.

Disclaimer

The information provided in this disclosure is provided "as is" without warranty of any kind. 1E disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall 1E or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if 1E or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the preceding limitation may not apply.