RBS-2018-002

combit List & Label Default Installation Folder Insecure Permissions Local Privilege Escalation

Vendor / Product Information

combit is a German company that offers products in the reporting, BI, and CRM markets for both small and large businesses. One of the products offered in the reporting space is the List & Label reporting tool, which is reportedly used by thousands of software development teams worldwide.

Vulnerable Program Details

Details for tested products and versions:

Vendor:	combit
Product:	List & Label
Version:	18, 19, 20, 21, 22, and 23

NOTE: Other versions than the ones listed above are likely affected.

Credits

Carsten Eiram, Risk Based Security
Twitter: @RiskBased

Vulnerability Details

combit List & Label installs to a child directory of %ProgramFiles%, which normally results in proper permissions being inherited to prevent trojaning attacks. However, the installer overwrites these permissions with insecure ones i.e. granting "Full Control" to "Everyone". This allows any local, unprivileged attacker on the system to plant or overwrite arbitrary files in the installation folder, which includes overwriting critical development components that may be bundled by other applications developed using the reporting tool.

Solution

The vendor has released a Service Pack, which sets proper permissions for certain critical sub-folders.

References

RBS:	RBS-2018-002[1]
VulnDB:	172996

Timeline

2017-11-16	Vulnerability discovered.
2017-11-16	Vulnerability reported to the vendor.
2017-11-17	Response received from the vendor.
2018-01-16	Service Pack released by the vendor.
2018-01-17	Alert sent to RBS VulnDB clients.
2018-03-22	Publication of this vulnerability report.

[1] https://www.riskbasedsecurity.com/research/RBS-2018-002.pdf

About Risk Based Security

Risk Based Security offers clients fully integrated security solutions, combining real-time vulnerability and threat data, as well as the analytical resources to understand the implications of the data, resulting in not just security, but the right security.

Company History

Risk Based Security, Inc. (RBS) was established to support organizations with the technology to turn security data into actionable information and a competitive advantage. We do so by enhancing the research available and providing a first of its kind risk identification and evidence-based security management service.

As a data driven and vendor neutral organization, RBS is able to deliver focused security solutions that are timely, cost effective, and built to address the specific threats and vulnerabilities most relevant to the organizations we serve. We not only maintain vulnerability and data breach databases, we also use this information to inform our entire practice.

Solutions

VulnDB - Vulnerability intelligence, alerting, and third party library tracking based on the largest and most comprehensive vulnerability database in the world. Available as feature-rich SaaS portal or powerful API. Vendor evaluations including our Vulnerability Timeline and Exposure Metrics (VTEM), Cost of Ownership ratings, Code Maturity, and Social Risk Scores.

Cyber Risk Analytics - Extensive data breach database including interactive dashboards and breach analytics. Clients are able to gather and analyze security threat and data breach information on businesses, industries, geographies, and causes of loss. It also allows monitoring of domains for data breaches and leaked credentials as well as implementing a continuous vendor management program with our PreBreach data.

YourCISO - Revolutionary service that provides organizations an affordable security solution including policies, vulnerability scans, awareness material, incident response, and access to high quality information security resources and consulting services.

Vulnerability Assessments (VA) and Pentesting - Regularly scheduled VAs and pentests help an organization identify weaknesses before the bad guys do. Managing the most comprehensive VDB puts us in a unique position to offer comprehensive assessments, combining the latest in scanning technology and our own data. Detailed and actionable reports are provided in a clear and easy to understand language.

Security Development Lifecycle (SDL) - Consulting, auditing, and verification specialized in breaking code, which in turn greatly increases the security of products.