

## Code B\_2754

<b>Department</b>	Electrical and Electronic Engineering
<b>UniCa reference person</b>	Davide Maiorca
<b>Project title in English</b>	Analysis of advanced software vulnerability exploitation techniques
<b>Project title in Italian</b>	Analisi di tecniche avanzate di sfruttamento di vulnerabilità nei software
<b>Subject area of reference (World University Ranking)</b>	ENGINEERING AND TECHNOLOGY
<b>Project summary and VPS' profile</b>	<p>Attackers often employ software vulnerabilities to compromise the integrity and availability of computer systems, either traditional (e.g., Desktop) or phones. Over the years, miscreants have progressively developed various techniques to exploit such vulnerabilities, thus even managing to control the target systems completely. For this reason, it is of utmost importance to understand such techniques in detail to develop proper defenses.</p> <p>The project aims to explore advanced exploitation techniques (for example, Return Oriented Programming) based on memory corruption bugs. Notably, while these techniques are widespread in Intel-based architectures, their application to RISC architectures (e.g., ARM) defines new challenges that should be addressed.</p> <p>The candidate VPS is supposed to have a wide knowledge of memory errors and exploitation techniques for various architectures (Intel, ARM, etc.), which is also reflected by a coherent research profile regarding selected publications.</p>
<b>Proposed length of stay</b>	Short visit of 6 days
<b>Expected period of activity</b>	July 2024
<b>Academic position of the VPS'</b>	Professor
<b>Course of Study</b>	Laurea magistrale (2nd cycle University Degree), Dottorato di ricerca (PhD Course)
<b>Language of instruction</b>	English