EPrints Security Review

Version:	1.0
Released:	1st March 2021

Contents

1 Executive summary

1.1 Background

EPrints is a free and open-source software package for building open access repositories that are compliant with the Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH)[1]. It shares many of the features commonly seen in document management systems, but is primarily used for institutional repositories and scientific journals. EPrints has been developed at the University of Southampton School of Electronics and Computer Science and released under a GPL license[2].

We estimate there to be at least 700 registered EPrints archives on the Internet[3]. Simple Google hacking (e.g. intext:"powered by eprints 3") reveals more unregistered instances, including some hosted under high authority domains. The EPrints software distribution site is itself an instance of EPrints[4].

A small team based at the University of Cambridge conducted a short code review of the EPrints 3.4.2 release during January 2021.

1.2 Overall posture

Test coverage was relatively low, and far from complete. Due to time pressures, the testing team focussed their efforts on studying the behaviour of endpoints under the `/cgi` path. It was believed this path offered a generous threat surface to remote network attackers, and the results indicate this triage to have been an efficient strategy.

The greatest impact achieved was unauthenicated remote code execution, and the development of a highly reliable exploit to establish a reverse shell. While certainly intolerable in most environments, such a bug is particulary impactful where EPrints is being used to distribute software (i.e. there is the potential for supply chain compromise)[5].

1.3 Risk ranking/profile

Software, hardware and firmware vulnerabilities pose a critical risk to any institution operating a computer network, and can be difficult to categorize and mitigate. The Common Vulnerability Scoring System (CVSS)