UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00148

HEWLETT PACKARD ZERO-DAY RCE FLAW

DATE ISSUED: 31st May 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A zero-day Remote Code Execution (RCE) flaw disclosed in December 2020, present in Hewlett Packard Enterprises (HPE) System Insight Manager (SIM) software, tracked as CVE-2020-7200 (rated 9.8/10), has been now been fixed since the release of the hotfix kit in April.

BREAKDOWN

The HPE SIM toolset allows for remote automation and management for a range of servers, storage and networking products, including the ProLiant Gen9 and Gen10. The vulnerability exists in the latest version (7.6.x) and only affects the Microsoft Windows version. By exploiting the hpsimsvc.exe process – which runs with administrative privileges, attackers would be able to execute code remotely without the requirement of any user interaction using low-complexity attack methods. There is a validation failure during the deserialization process when a user submits a POST request through /simsearch/messagebroker/amfsecure and attackers are able to leverage an outdated copy of the Commons Collection (3.2.2) and can lead to the deserialization of untrusted data, therefore allowing RCE.

REMEDIATION STEPS

- Update affected devices to deploy the security patch.
- Use the Hotfix kit supplied by HPE if you are unable to apply the latest updates straight away.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/hpe-fixes-critical-zero-day-sim/166543/
E-Hacking News	https://go.newsfusion.com//security/item/1868841
HP Support Center	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04068en_us
Packet Storm	https://packetstormsecurity.com/files/161721/HPE-Systems-Insight-Manager-AMF-Deserialization-Remote-Code-Execution.html