National Cyber Security Centre

IR-18122019-NCSC

A part of **Department of Communications, Climate Action & Environment**

CSIRT-IE Advisory

HPE SAS SSD Vulnerability

Status: TLP-WHITE

Traffic Light Protocol

This document is classified using Traffic Light Protocol. Recipients may share TLP: WHITE information freely, without restriction. For more information on the Traffic Light Protocol, see `https://www.first.org/tlp/` Please treat this document in accordance with the TLP assigned.

Technical Details

The Computer Security Incident Response Team - Ireland (CSIRT-IE) is a unit in the National Cyber Security Centre, hosted by the Department of Communications, Climate Action and Environment. Please find below the details of our latest advisory.

1. Overview

Threat Type	Vulnerability
Systems Affected	HPE SAS SSDs with firmware older than HPD8
Impact	Drive failure and data loss
Recommendations	Upgrade to latest version of firmware

2. Description

Hewlett Packard Enterprise (HPE) has released a firmware update for some of its branded SSDs which fixes a critical vulnerability. This vulnerability will result in drive failure and data loss at 32,768 hours of operation.

Full details are available from HPE at `https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00092491en_us`. This firmware defect affects certain SAS SSD models used in a number of HPE server and storage products including HPE ProLiant, Synergy, Apollo, Synergy D3940 Storage Mod-

ule, D3000/D6000/D6020 Disk Enclosures, MSA Storage, StoreEasy 1000 Storage, StoreVirtual 4335 Hybrid Storage and StoreVirtual 3000 Storage.

HPE's advisory states that if several disks have been installed at the same time, this may lead to failure at approximately the same time. In the worst case, the disks become unusable and the associated data can no longer be read. It should be noted that the HPE advisory states: "By disregarding this notification and not performing the recommended resolution, the customer accepts the risk of incurring future related errors."

3. Mitigation

All HPE SAS SSDs with firmware older than HPD8 will be affected by the software error. According to HPE, a firmware upgrade to HPD8 will address the vulnerability. The HPE bulletin contains details of how to apply this critical fix and instructions on how to determine how many hours SSDs have been on. Links to downloadable updates etc. are also provided. Updates to some versions are still awaited.

Users can check their own disk system by using the Smart Storage management interface. A sample command to check total system hours, models etc. can be seen below:

```
$ ./ssacli ctrl slot = 0 ssdphysicaldrive all show | awk '/ physicaldrive
\\/ {print $ 2}' | xargs -I% ./ssacli ctrl slot = 0 pd% show | awk '/ Power On Hours
\\/ || / physicaldrive / || / Firmware / || / Model / {print} '}
```

CSIRT-IE urges caution when interacting with Smart Storage Management interface. These commands should only be run by an experienced Systems Administrator. CSIRT-IE is not liable for any unexpected events as a result running the above command or similar commands.

Due to the potential for data loss CSIRT-IE encourages all constituents to urgently address this vulnerability.

Feedback and Reporting

NCSC and CSIRT kindly requests any feedback users may wish to provide in relation to this advisory as regards the relevance and accuracy of the information provided. Feedback can be provided by emailing info@ncsc.gov.ie or certreport@dccae.gov.ie.