高性能计算（HPC）桌面演习指南

CSA GCR cloud security GREATER CHINA REGION alliance®

CSA cloud security alliance®

物联网工作组官方地址是：

https://cloudsecurityalliance.org/research/working-groups/internet-of-things/

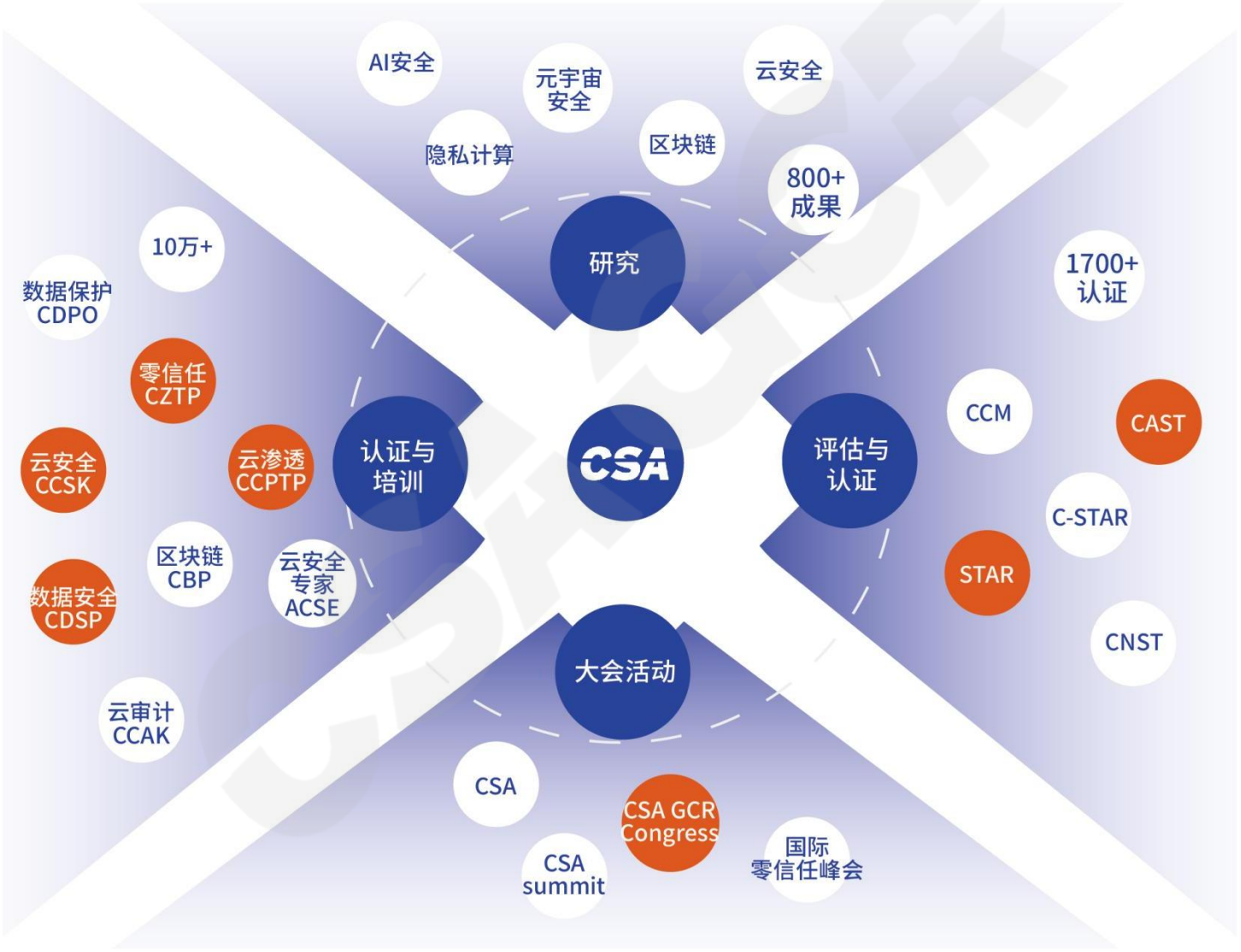
联盟简介

云安全联盟（Cloud Security Alliance,CSA）是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区（Cloud Security Alliance Greater China Region, CSA GCR）作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

我们的工作

联盟会刊下载地址
了解联盟更多信息



加入我们

CSA大中华区官网
（https://c-csa.cn）

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

致谢

报告中文版支持单位

浪潮云是中国最早提供云服务的厂商之一（2010），是首批国家机关云服务提供商。作为中国行业云的引领者，浪潮云致力于成为高品质云服务提供商，具备“专业、生态、可信赖”三大核心优势。为客户提供云网边端融合、云数智融合、建管运融合的全栈云服务，构建零信任的云数安全体系，打造新一代混合云。携手合作伙伴，共建云舟联盟生态，支撑政府、企业数字化转型，助力数字中国建设。

浪潮云是 CSA 全球会员单位，支持该报告内容的翻译，但不影响 CSA 研究内容的开发权和编辑权。

英文版本编写专家

主要作者：

Jim Basney　　Christopher Frenz　　Michael Roza　　Brian Russell

贡献者：

Pedro Cabezas　　Kenny Chu　　Joseph Louis-Jean　　James Murphy

Kristin Myers　　Gary Schaefer　　Rishi Tripathi

审校者：

Ashish Vashishtha

CSA 员工：

Hillary Baron　　Claire Lehnert

在此感谢以上专家。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给予雅正！联系邮箱 research@c-csa.cn；国际云安全联盟 CSA 公众号。

序言

随着工业 4.0 和人工智能等技术的发展，高性能计算（HPC）系统在制造业和人工智能中也得到了创新性的发展，如在制造业中，利用 HPC 系统进行高精度的数值模拟来优化设计方案，减少实验成本；在人工智能中，利用 HPC 进行深度学习、大规模数据分析和机器学习等任务，以提高人工智能的效果和性能。HPC 在快速发展和应用的同时，其安全风险和漏洞也逐渐得到关注，特别是 HPC 计算集群，成为了加密挖矿掘恶意软件的黑客组织的理想目标。

随着越来越多的 HPC 系统应用面向终端用户开放，提供互联网接入服务，针对 HPC 系统的网络攻击也逐渐增多。然后针对 HPC 系统安全的防护却有待进一步加强，目前大部分 HPC 系统在 IT 部门之外处理，通常由专门从事 HPC 系统的个人管理，可能缺乏正式的网络安全培训和网络攻防实战经验，导致 HPC 系统一旦被攻击，其发现、响应、处置和溯源等安全流程将变得更加模糊与困难。

本白皮书以专业的视角，从 HPC 系统的网络安全桌面推演出发，详细阐述了 HPC 系统的架构、HPC 系统安全桌面推演中的各方角色、场景构建和注意事项等，给读者提供了一个详细可落地的高性能计算 HPC 系统网络安全桌面推演方案，以帮助 HPC 系统安全管理人员快速获取网络安全及攻防相关经验，提升 HPC 安全管理人员的网络安全响应和处置水平。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

1.简介

虽然新闻中广泛报道了突出的勒索软件攻击和影响组织的大规模数据泄露事件，但你并不经常读到这些攻击中的一个对高性能计算(HPC)系统的影响。因此，HPC 系统的风险和漏洞是一个在安全对话中经常被低估的领域。虽然在直接与 HPC 环境打交道的安全社区之外，并不经常讨论 HPC 计算机系统作为网络攻击目标的潜力，但在攻击者圈子里并没有被忽略。特别是，HPC 计算集群被认为是寻求部署加密挖矿掘恶意软件的黑客组织的理想目标。

HPC 系统的安全性通常代表了关于组织内如何普遍管理 HPC 系统的有趣挑战。在许多计算中心，HPC 系统是在组织的 IT 部门之外处理的，通常由专门从事 HPC 系统的个人管理，可能缺乏正式的网络安全培训。同样，大多数组织内的网络安全团队可以带来专门的网络安全知识，但可能缺乏 HPC 环境的正式培训，以及缺乏对 HPC 架构与更传统的独立 Linux/Unix 服务器的设置有何不同的了解。当你把那些经常编写应用程序在 HPC 系统上运行的研究人员加入进来，他们可能缺乏 HPC 系统管理或应用程序安全方面的正式培训，围绕如何开始保护这些 HPC 系统的讨论迅速变得非常模糊。

然而，这是一个重要的讨论，特别是当越来越多的 HPC 应用被发现有一个基于网络的前端，允许用户与运行在后端的 HPC 分析应用进行互动。随着各行业对大数据分析、机器学习、人工智能(AI)和其他此类应用的进一步使用，越来越多的 HPC 应用正在获得一个面向公众的前端。在这样做的时候，它使 HPC 应用失去了传统上保持其安全的仅有内部可访问性的保护。针对 HPC 应用的攻击可能会增加，因此企业必须在针对 HPC 系统的攻击变得更加普遍之前，就保护 HPC 系统的安全进行探讨。

本指南列出了举办以 HPC 为重点的网络攻击桌面演习(TTX)所需的框架，以便组织能够为 HPC 安全进行规划。本指南通过一个 TTX 的例子，帮助利益相关者在事件发生时讨论 HPC 的安全问题，为改善 HPC 系统的安全而采取的行动建立共识，并围绕 HPC 系统制定事件响应(IR)流程。

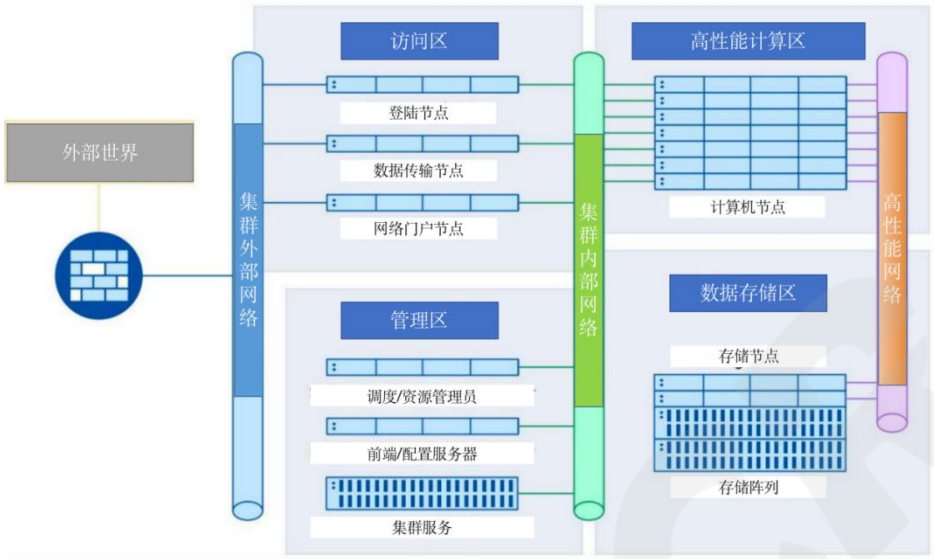
利益相关者

为了在 HPC 安全方面达成共识并建立共同的目标，来自以下组织领域的代表应参加 TTX。

> - 行政领导
> - HPC 系统管理
> - 网络安全/信息安全
> - HPC 应用开发者
> - 利用 HPC 环境的研究人员信息技术
> - 事故应对人员/取证
> - 法律
> - 媒体关系

在利益相关者参与 TTX 和情景展开的过程中，必须牢记 TTX 不是一个挑战，目的是以确定一个组织内的安全状况有多好,因此、利益相关者不应该因为某些控制措施的存在而争论该场景的可行性。桌面演习假设控制失败，以引导组织全面了解其事件响应(IR)流程，并作为一种识别额外补偿控制的方式，在控制失败的情况下应该有所帮助。

2. HPC 架构



HPC 系统是复杂的、不断发展的，因此一个通用的词典可以帮助描述和识别 HPC 系统的架构、关键元素、安全威胁和潜在风险。上面的架构概述是基于 NIST SP 800-223 高性能计算标准草案。

一个有代表性的 HPC 架构通常由以下网段组成：

外部世界：外部世界是指互联网或其他完全处于 HPC 环境之外的组织网络。在本桌面演练指南中，外部世界将是互联网，对网络服务器的请求由此开始。

集群外部网络：外部世界通常通过防火墙与群集外部网络分开。集群外部网络是连接到访问区公开访问资源的所有接口的地方。

集群内部网络：集群内部网络是一个内部网络段，它将访问区、管理区、高性能计算区和数据存储区的组件相互连接。在本桌面演练指南中，内部防火墙被用来将访问区的资源与其他区的资源分开。

高性能网络：高性能计算网络用于互联高性能计算区的各个节点，以及连接高性能计算区和数据存储区的资源。该网段通常被设计为高速运行，并具有低延迟。

一个 HPC 系统被划分为四个功能区：

- 访问区
- 管理区
- 高性能计算区
- 数据存储区

访问区

访问区包含一个或多个连接到外部网络的节点，如互联网或其他组织网络。这个区域提供对用户和管理员访问和连接进行认证和授权的能力。访问区为使用各种服务提供便利，如交互式 shell、基于网络的门户、数据传输和数据可视化。

管理区

管理区由一个或多个管理节点及云服务集群组成，提供 HPC 管理服务。这个区域允许 HPC 系统管理员执行管理操作，如配置和调配计算节点、存储和网络。此外，这个区域可以被用来执行身份管理、漏洞管理和系统审计。它还可以被利用来允许用户在通过访问区成功认证和授权后请求计算和存储服务的接口。管理软件模块，如作业调度器，在管理区运行。

高性能计算区

高性能计算区是由高速网络连接的池状计算节点组成的。这个区域提供的服务对大规模运行并行计算工作至关重要。

数据存储区

数据存储区由一个或多个高速并行文件系统组成，为用户数据提供数据存储。这些文件系统被设计用来存储非常大的数据量，并提供高速读写操作。

3.概述

桌面演习(TTX)是在一个非正式的、无压力的环境中，根据目前适用的政策、计划和程序，促进对脚本情景的讨论。TTX 的目的是促进对概念的理解，确定优势和劣势，并为政策和程序的改变提供建议。

TTX 的主要阶段和产出介绍如下：

演习规划小组

演习计划小组(EPT)对任何演习的成功都至关重要。该小组应在演习前三个月选定。规划小组的职责包括但不限于:

- 获得领导层/管理层的认同引导发展进程
- 获得资源
- 安排和协调
- 确定演习的范围
- 确定目标
- 确定参与者
- 开发 TTX 材料(即讲义、幻灯片、表格)

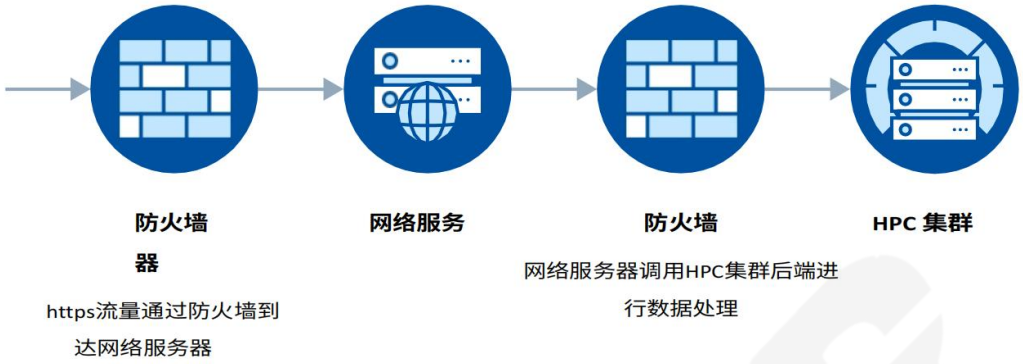
规划小组应仔细挑选，由可能受影响的业务单位的代表组成。该小组应具有可管理的规模，不应成为演习的参与者。对 EPT 成员的建议包括：

- 行政领导
- HPC 系统管理
- 网络安全/信息安全
    - HPC 应用开发者
    - 利用 HPC 环境的研究人员信息技术
    - 事故应对人员/法医
    - 法律
    - 媒体关系

在进行网络安全桌面演练时，至关重要的是，参与演练的不仅仅是网络安全和团队。网络安全事件有可能影响到网络安全和 I 以外的业务部门的运作，在事件应对计划中需要考虑到这些业务部门的需求，以确保尽可能地减少对业务的影响。恢复和响应需要许多功能和人员您计划中的一些合作伙伴可能是外部的。为了有效测试响应和恢复计划，应该让各种内部和外部团队参与进来。

当决定让利益相关者参与演习时，还必须考虑到桌面演习活动可以作为提高对安全问题以及它们如何影响业务的认识的重要手段。建立一个有效的安全计划需要网络安全和 I 以外的利益相关者的支持和认同。桌面演习是一个很好的方式来说明在网络安全事件中可能出现的操作问题，并因此获得不同利益相关者的支持和认可。桌面演习可以帮助缩小差距，提高对有效的网络安全在 HPC 环境中的重要性的认识。

4.桌面演习场景的开始



这个桌面演习是围绕一个 HPC 系统进行的，该系统有一个基于 Web 的前端(访问区)，允许应用程序的用户将数据提交给 HPC 集群进行处理。网络服务器由防火墙保护，只允许 HTTPS 流量通过。网络服务器与 HPC 集群被另一个防火墙隔开，该防火墙只允许网络服务器与 HPC 集群之间的互动所需的流量通过。高性能计算、数据存储和管理区都在这第二道防火墙后面。该架构保持最小化，以使桌面练习更普遍地适用于利用 HPC 的各种组织。

那是一个星期二的早上 9 点半，HPC 管理员与 I 部门合作，为上线一个新的基于网络的应用程序做最后的润色。该应用程序使用该组织的一个 HPC 系统作为一种新形式的基因序列比对的后端，这使得生物信息学研究界有了一种识别基因序列相似性的增强方式。该应用程序允许研究人员以文件的形式上传基因序列，然后将其与数百万其他基因序列进行比较，以比传统算法(如基本局部排列搜索工具(BLAST))更高的速度和保真度找到匹配。

需要考虑的问题：

1. 该组织是否有编写 HPC 应用程序或其网络前端的开发人员接受过应用程序安全方面的培训?
2. 该组织是否制定了安全应用开发的标准，明确规定了输入验证、转义和其他关键应用安全控制的需要?

3. 组织是否授权在应用程序上线前进行任何形式的安全测试?

   a.静态应用安全测试(SAST)?

   b.动态应用安全测试(DAST)?

   c.渗透测试?

4. 组织是否有一个正式的计划来维护已发布的应用程序，包括报告和补救安全问题？

5. 您的组织是否有一个正式的 DevSecOps 方法，类似于 CSA 的《DevSecOps 的六大支柱》中描述的方法?

注入 1

两周后，下午 3:30，内部和外部研究人员开始报告说序列排列应用程序的性能很差。一位 HPC 系统管理员检查了这个问题，并报告说 HPC 集群上的 CPU 和内存使用率特别高。管理员报告说进程"kworkerds"对高资源利用率负责。管理员还指出，连接到 HPC 系统的网络连接看到比预期更高的利用率。

需要考虑的问题：

1. HPC 集群上有什么样的性能监测?
2. 是否有性能基线可以帮助使这个问题更容易被发现?
3. 什么是 kworkerds?这个过程的名称有什么突出的地方吗?
4. 是否有一个关于哪些进程应该在 HPC 系统上运行的基线，以便更容易识别运行中的未经批准的进程?
5. 此时应该考虑安全事件，并通知信息安全团队，还是由 HPC 系统管理团队进行初步调查?
6. 在 HPC 系统上是否安装了任何安全软件来检测恶意进程，或者由于性能原因而避免了这一点?

7. 是否有适当的日志记录，以帮助调查和找到这样的问题的根本原因?
8. 来自 HPC 环境的日志是否进入了安全信息和事件管理(SIEM)系统?
9. 在 HPC 系统周围是否存在任何出口过滤控制?

注入 2

HPC 系统团队继续调查这个问题，在根账户的主目录中，一位管理员发现了一个名为 ransomnote.txt 的文件。管理员打开该文件，看到的信息是：”与超人不同，你的超级计算机并不是无敌的。你的研究数据已经被盗，并将被公布给你的竞争对手，除非你允许我们挖出 100 个比特币。如果我们的矿工在挖到 100 个比特币之前被停止，你的数据将被公开。当 100 个比特币被挖出来后，我们的矿工将终止并删除自己"。

需要考虑的问题：

1. 如果上面还没有决定，现在的问题是安全事件吗?
2. 谁会是这个问题的事件指挥官?
3. 是否有处理 HPC 事件的现有事件响应(IR)计划?
4. 将采取什么措施来控制事件并阻止组织内的其他系统被破坏?
5. 为调查这个问题，会做些什么?
6. 组织是否有调查所需的数据(例如，记录的全面性)和资源(专业知识、工具等)?
7. 什么样的数据可以从超级计算环境中获得?
8. 可能被外流的数据被公开的潜在危害是什么?
9. 网络分段是否到位，或者数据是否有可能从环境的其他部分被访问和渗出?
10. 这个时候法律团队是否参与其中?

11. 是否会通知执法部门?

12. 组织中还有谁需要被通知这一事件?

13. 该组织是否会考虑通过保留安装的密码挖掘机来"支付"赎金?

注入 3

第二天，一个著名的勒索软件集团在他们的博客上声称对这次攻击负有责任，新闻机构开始给员工打电话并提出问题，因为这次攻击的新颖性使得它具有新闻价值。其他组织的研究合作者正在询问有关被渗出的数据和暴露的研究机密的问题。一些合作者威胁说，如果他们不尽快得到答案，他们将终止合作并将研究资金转移到其他地方。

需要考虑的问题：

1. 如果还没有，法律、执法或任何其他利益相关者是否会参与?
2. 该组织是否会就袭击事件发表公开声明?
3. 如果有的话，会向威胁要撤消其研究经费的合作者传达什么?
4. 这一新信息是否对支付赎金或不支付赎金的决定有任何影响?

注入 4

事件发生后的几个星期，取证调查已经完成。经确定，文件上传功能中的一个不安全因素被利用了，这使得前端网络服务器被入侵。从那以后，攻击者能够利用传递给 OpenMP API 调用的数据缺乏输入验证和消毒的情况，以便将恶意软件注入共享内存，并在 HPC 集群的各节点上传播加密机器。

需要考虑的问题：

1. 如何才能更好地保护前端 Web 服务器免受类似的攻击？
2. 漏洞管理是保护信息系统的关键，因为它可以确保这些系统有最新的补丁，但 HPC 系统运行各种特殊的库和软件包，商业漏洞扫描器可能没有

签名。由于缺乏补丁，也许甚至无法识别需要补丁的地方，如何才能减轻 HPC 系统的风险？

3. 是否有一个用于 HPC 系统的开源软件的清单？

4. 端点安全工具、扩展检测和响应(XDR)工具、SIEM 工具等等，都有可能检测到恶意行为，但大多数都是围绕 Mitre ATT&CK 和其他在对客户的攻击中经常观察到的恶意行为进行检测。商业安全工具是否能提供所需的检测，围绕着是 HPC(MPI，OpenMPI 等)特有的可利用方面，还是会有一个盲点，除非建立自定义的检测？

5. 重新考虑围绕开发人员的应用安全培训和安全软件开发的其他方面的问题，根据上述考虑，你现在的答案是否有所不同(缓解漏洞的最好方法是首先防止它被引入)？

6. 这是一个常见的应用安全格言，你必须在其中建立安全，而不是把安全栓在上面还有哪些方法可以更好地将安全建立在 HPC 系统和我们在其上运行的应用程序中？

7. 鉴于 HPC 应用经常依靠 C/C++或 Fortran 等”内存不安全”语言编写的代码来达到性能目的，HPC 世界是否应该考虑开始转向像 Rust 这样具有类似性能的更多内存安全语言？

参考文献

- 欧洲各地的超级计算机被加密货币开采恶意软件攻陷。Sabina Weston，ITPRo.(2020 年 5 月 18 日).
- h t t ps://www.it pro.com/security/malwa re/35 5 6 7 7/uni-of-e d i n b u r g h-s u p e r c o m p u t e r-t a k e n 被加密货币挖掘的恶意软件所击倒
- 通过一个自定义的网络界面提交你的 HPC 工作。AWS(2021)
- https://awslabs.github.io/scale-out-computing-on-aws/web-interface/submit-hpc-jobs-web-based-interface/
- 用于高性能计算的网络门户：一项调查。Patrice Calegari，Marc Levrier，and Pawet Balczynski.(2019 年 2 月)。
- https://dl.acm.org/doi/pdf/10.1145/3197385
- NIST,SP 800-223(草案)高性能计算(HPC)安全：架构、威胁分析和安全态势(2023 年 2 月草案，评论期截止到 2023 年 4 月)
- https://csrc.nist.gov/publications/detail/sp/800-223/draft
- 云安全联盟(CSA)，远程手术桌面指南书，物联网工作组、发布日期:01/30/2023
- https://cloudsecurityalliance.org/artifacts/telesurgery-tabletop-guide-book/
- 云安全联盟(CSA)，云事件响应框架，云事件响应工作组，发布日期：05/04/2021
  https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/
- BLAST,https://blast.ncbi.nlm.nih.gov/Blast.cgi

CSA GCR cloud security alliance
GREATER CHINA REGION ®

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网：https://c-csa.cn 电话：0755-86548359
地址：上海市浦东新区东育路255弄5号3FB30（前滩国际经济组织集聚区）/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905