关于发展中国安全浏览器的建议

Suggestions on Developing China's Secure Browsers

魏小强/WEI Xiaoqiang，张义荣/ZHANG Yirong，
黄亚洲/HUANG Yazhou

（360数字安全集团，中国 北京 100102）
(360 Digital Security Group, Beijing 100102, China)

DOI：10.12142/ZTETJ.202301010
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20230222.1735.006.html
网络出版日期：2023-02-23
收稿日期：2022-11-05

摘要：安全浏览器是数字工作空间的安全入口。通过对全球安全浏览器发展趋势的洞察，分析中国在安全浏览器领域所面临的机遇与挑战，提出通过发展中国安全浏览器来构建中国关键数字安全能力的建议。认为应鼓励政企单位使用国产安全浏览器，培育安全浏览器社区文化，加强安全浏览器人才培训。

关键词：安全浏览器；风险；数字工作空间；微软；谷歌；人才培训

Abstract: The secure browser is a secure portal of digital workspaces. Through the insight into the development trend of global security browsers, the opportunities and challenges faced by China in the field of security browsers are analyzed, and suggestions for building China's key digital security capabilities by developing China's security browsers are put forward. It is believed that government and enterprise units should be encouraged to use domestic security browsers, cultivate security browser community culture, and strengthen security browser talent training.

Keywords: secure browser; risk; digital workspace; Microsoft; Google; talent training

安全浏览器已经成为数字工作空间的安全入口。安全浏览器也将成为在操作系统之上保护数字工作空间的新操作系统。微软放弃开发26年之久的网页浏览器（IE），转而拥抱竞争对手谷歌的Chromium开源浏览器内核项目并推出新Edge浏览器（目前排名全球第4）。这进一步刷新了行业对Chromium的认知，也使得跨平台、标准化、统一性、拥抱开源的安全浏览器迅速成为热点。从以色列安全浏览器初创公司Talon Cyber Security获得2022年RSAC创新沙盒冠军，到刚刚成立两年的企业级安全浏览器厂商Island一跃成为估值最高的独角兽企业，以及资本市场对安全浏览器的热烈追捧，可以看出，安全浏览器将推动安全行业的深刻变革。

在俄乌冲突之际，美国网络安全和基础设施安全局（CISA）在2022年2月份发布的“屏蔽”计划（Shields-UP）指出，“每个组织，无论大小，都必须准备好应对破坏性的网络事件……更新手机、平板电脑和笔记本电脑上的操作系统，并更新所有设备上的应用程序——尤其是网络浏览器”[1]。这进一步证明了安全浏览器不仅是数字工作空间的安全入口，也已经成为国家网络防御的前沿阵地。此外，CISA还表示，“利用Web浏览器中的漏洞已成为攻击者破坏计算机系统的一种主要方式”。由此可见，Web浏览器的战略意义已经从为消费者提供互联网“冲浪”的入口变成构建国家网络防御能力的前沿阵地。随着全球加速进入数字时代，数字工作空间无处不在，保护数字工作空间的第一道门户——安全浏览器很可能是未来安全行业的游戏规则改变者。

1 现有网络浏览器存在巨大安全风险

网络浏览器是人们日常使用的用来检索、展示以及传递Web信息资源的应用程序。随着互联网的飞速发展，网络浏览器已成为人们使用最多的应用程序。它不仅是一个互联网访问入口，还是用户业务、资产、信息的接入枢纽。目前，网络浏览器已经发展为新一代数字工作空间，即用户进入互联网空间的访问入口。但是，它并不是为安全而设计的。Chrome、Firefox等浏览器已成为黑客渗透攻击的重要目标，也是许多高级持续威胁（APT）组织常用的攻击入口。近年来，受新冠疫情影响，自带设备（BYOD）办公方式被众多组织大量使用，导致网络浏览器所面临的安全问题更加突出。

1.1 网络浏览器充斥大量易被黑客利用的漏洞

谷歌 Chrome、微软 Internet Explorer、Mozilla Firefox 和 Apple Safari 等网络浏览器安装在几乎全球所有的计算机上。据 Statcounter 数据显示，谷歌 Chrome 浏览器以 63.63% 的份额（拥有 33 亿用户）引领网络浏览器市场；Apple Safari 紧随其后，份额为 19.37%；Mozilla Firefox、微软 Edge（Chromium）、Opera、Internet Explorer 的份额分别为 3.65%、3.24%、2.16%、0.81%[2]。

操作系统附带的网络浏览器往往采用默认的安全设置，例如：Chrome 和 Safari 这样的网络浏览器很容易受到跟踪、恶意工具栏和插件的影响，在其外挂的工具栏和插件中，充满了公共漏洞（CVE），从而使得这些浏览器成为黑客最喜欢的攻击目标。网络攻击者经常利用浏览器上的安全漏洞来窃取机密数据，安装勒索软件并策划网络攻击。

CVE 详情报告显示，所有 4 个主要浏览器在 CVE 方面均排在前 25 位。其中 Chrome 浏览器排在第 9 位，有 2 346 个 CVE；Firefox 排在第 13 位，有 1 933 个 CVE；Internet Explorer 排在第 24 位，有 1 168 个 CVE；Safari 排在第 25 位，有 1 136 个 CVE。Microsoft Edge 于 2015 年亮相，迄今有 250 个 CVE，因此没有进入前 25 位[3]。

统计数据显示，超过 9% 的 Chrome 浏览器扩展功能权限具有高风险或极高风险。2021 年的 Chrome 因被发现 308 个 CVE 而被评为最易受攻击的浏览器。其中，24% 的零日漏洞与 Chrome 有关。由通用漏洞评分系统（CVSS）评估的 Chrome CVE 的风险值（6.4）高于所有其他应用的 CVE 平均值（6）。其他网络浏览器的情况和 Chrome 类似，这里不再赘述。

综上所述，网络浏览器已经成为最容易被攻击的应用程序。然而，企业或机构正在广泛使用网络浏览器来访问其业务应用环境。也就是说，全球有数十亿人的数字工作空间门户正面临着巨大的安全风险。

1.2 网络浏览器缺乏企业级应用所需的安全性设计

Chrome 等网络浏览器往往是为消费者、广告商、内容生产者和开发者而构建的，它也会通过广告、用户跟踪和搜索优化等方式来盈利。因此，面向消费者的浏览器很容易受到网络攻击。比如，攻击者可以遍历浏览器标签，以了解有关受病毒感染主机的丰富信息；通过读取保存用户名和密码的特定文件来获取用户账号信息；利用浏览器安全漏洞和固有的浏览器功能来更改内容，修改用户行为，获取终端系统的最高访问权限并完成横向移动，拦截信息并进行会话劫持；滥用浏览器扩展功能来实现对被攻击者应用系统的持续访问与机密数据获取等。

网络浏览器之所以容易受到上述网络攻击，是因为它并不是为企业级安全性需求而设计的。企业在使用浏览器时会遇到 3 个非常重要而且经常被低估的问题：可见性、可控性和可管理性问题，即企业无法获知用户的访问行为、访问的目的地、访问的风险性、具体的操作行为等。

1.3 非受控端广泛采用网络浏览器进一步加剧企业安全风险

根据美国市场研究公司 Forrester 的一项调查，69% 的受访者声称其网络上一半或更多的设备是 BYOD 等非管理设备或物联网设备[4]。这些设备往往通过网络浏览器接入和访问企业的各种资源。

当 BYOD 访问企业资源时，企业无法在员工自带设备上部署企业级安全策略，而网络浏览器是此类非受控端点接入和访问企业应用的主要途径。这将进一步加剧安全风险，使得企业无法完全对访问内容进行安全控制。事实上，大多数企业的安全团队根本无法验证访问企业资源的非企业设备的安全状况。

但是，BYOD 工作的方式越来越受欢迎，物联网设备正在爆炸性增长。这是数字时代的基本特征。那么如何帮助企业 IT 和安全部门对这些设备实现安全可见性和控制能力？比较好的方法就是采取更轻量级的方式，比如使用安全浏览器等手段来增强可见性和可控性。

2 安全浏览器成为数字工作空间的安全入口和各国关注焦点

如果把网络浏览器比作一辆汽车，那么安全浏览器就是汽车安全气囊。全球数字化转型正在加速发展，为应对混合工作环境下的安全挑战，人们需要一种新的安全工具来保护数字工作空间。安全浏览器很可能将顺应历史潮流担当此任。随着浏览器正在朝着标准化、平台化和系统化演进，安全浏览器正在成为数字工作空间的安全入口和新防线。微软、谷歌以及资本市场等均在加速布局安全浏览器战略，抢占未来数字工作空间安全入口的控制权。

2.1 数字化转型需要新的安全工具来保护用户数字工作空间入口

数字化转型重塑了企业的交付服务和访问应用的方式。比如：BYOD 的广泛采用、企业上下游供应链之间的相互访问以及大量物联网设备的出现，导致企业或机构在混合工作方式下面临的网络攻击面急剧扩大。网络攻击者很容易采用多种方式针对分布式工作的用户发起攻击，例如：利用合作

方未修补的浏览器漏洞，通过浏览器下载的恶意软件，利用浏览器实施欺诈、网络钓鱼以及零日攻击等。传统安全手段仅仅保护可管理设备，无法收敛攻击面，同时还带来高延迟、高成本以及用户体验差等问题。

因此，企业必须找到并实施正确的解决方案，既要实现数据安全性、完全可见性和可控性，还要考虑在混合工作环境下不断提升用户体验等问题。这意味着需要创建一个跨平台、标准化、统一化、易于操作且可实施一致的安全态势管理策略的安全环境，并将其作为保护数字工作空间入口的关键。

随着企业不断把业务迁移到云上，越来越多的企业开始采用基于浏览器的软件即服务（SaaS）应用程序。那么，将安全性集成到浏览器中并创建基于安全浏览器的企业环境就成为一个轻量级的、用户体验良好的选择。安全浏览器的作用方式相当于在传统操作系统之上构建了一个新的基于浏览器的安全操作系统。因此，企业安全浏览器有望成为网络安全行业的“游戏规则改变者”。据统计，到2026年，支持分布式工作的网络解决方案市场规模预计将达到420亿美元[5]。毫无疑问，安全浏览器将是该解决方案中的核心组件之一。

2.2 微软推动Chromium发展，加大数字工作空间入口控制权的争夺

以微软为代表的巨头在Chromium开源内核方面不断发力。微软于2022年6月15日停止IE浏览器服务。该科技巨头果断放弃IE（截至2021年3月市场份额为1.7%），转而与竞争对手谷歌联合推出基于Chromium的Edge浏览器。很显然，该事件将极大地推动Chromium成为浏览器标准，加速行业关于Chromium的共识。

微软于2018年转向Chromium开源内核之后，并不是一个简单的Chromium的跟随者，而是投入其Edge团队的核心力量在Chromium上进行持续开发，并迅速成为全球仅次于谷歌的第二大Chromium开发团队[6]。虽然Edge和Chrome都基于开源Chromium内核，但是微软做了很多差异化的能力开发，基于Chromium底层技术做了很多性能优化，并且引入了人工智能和机器学习技术等，例如：其在Edge中构建所谓的“图灵图像超分辨率引擎”[7]，允许用户增强他们在Web上看到的图像，这使得使用微软的Edge浏览器比Chrome看起来更清晰；在安全能力方面，增加了Smart Screen的功能，能够帮助用户免受网络钓鱼、恶意软件站点和软件的侵害；为用户提供过滤机制，用机器学习智能提醒、过滤、防御钓鱼网站、有潜在危险的网站等[8]。微软Edge团队正在为Chromium开源社区做出巨大贡献，迅速成长为该社区的第二大力量，正在影响并可能引领该社区的发展[9]。

此外，微软还在资本市场收购安全浏览器领域的新锐企业和技术，如对Talon Cyber Security的扶植。以色列企业安全浏览器初创公司Talon Cyber Security获得了2022年RSAC创新沙盒冠军。该公司基于Chromium推出自己的企业安全浏览器产品。Talon Cyber Security在2022年6月与微软签署了排它性创业公司孵化计划，将获得微软的技术、能力和资源的支持。可以看出，微软正在借力Talon的安全浏览器技术扩大其企业安全浏览器战略，争夺数字工作空间入口的控制权。

事实上，目前资本市场对安全浏览器领域表现出极高的兴趣。我们注意到，最近两年涌现出了一些独立的安全浏览器厂商，比如：另一家以色列安全浏览器公司Island，在2022年3月完成B轮融资，共筹集到1.15亿美元，以13亿美元的估值成为历史上首个估值最高的安全浏览器独角兽企业。该公司的主打产品也是基于谷歌Chromium内核的企业安全浏览器。

值得注意的是，当前，中国非常依赖微软IE的浏览器插件，例如：利用基于IE等标准浏览器兼容和扩展的一些国密产品的安全加密功能，来保护金融领域电子交易等。因此，微软放弃IE浏览器将对中国原有基于微软IE扩展的兼容加密技术的升级等产生重要影响。

2.3 谷歌发布Chrome企业连接器框架，加速布局安全浏览器战略

为了应对混合工作环境下的网络安全挑战，谷歌在其Chrome浏览器和Chrome OS的基础上，于2022年5月26日推出了Chrome浏览器和Chrome OS企业连接器框架（Chrome Enterprise Connectors Framework）。该框架主要在Chrome OS中为企业增强数据控制能力，从而更好地保护企业环境中用户和设备的安全，同时为安全团队提供更多工具来报告和管理安全事件。

目前约有10家硬件和安全头部企业响应谷歌这一框架计划，例如：英特尔推出vPro设备管理工具包，以加密Chrome OS设备的内存；Palo Alto Networks、CrowdStrike Holdings、BlackBerry统一终端管理（UEM）、VMware、Splunk以及三星Knox Manage等均承诺会尽快推出基于谷歌企业连接器框架的安全方案。

可以看出，谷歌正在借助合作伙伴的力量构建从芯片到云的全链路安全方案。企业安全浏览器作为数字工作空间的

入口具有举足轻重的战略意义。

3 相关建议

安全浏览器是构建在操作系统之上的操作系统，具有巨大的平台价值和极其重要的战略意义，需要我们高度重视。目前，针对中国浏览器使用情况的调研显示，中国安全浏览器在开发方面具有先发优势，但是也面临着很大挑战：人们还未认识到安全浏览器的重要战略意义，企业对安全浏览器的付费愿望不足，安全浏览器研发人才短缺等因素正在阻碍中国安全浏览器的发展。承载中国党政军企各类业务的系统均通过网络浏览器进行访问，浏览器的安全性已关乎到国家网络空间的安全。为加速推动我国安全浏览器的发展，我们提出3个相关建议。

3.1 发挥先发优势，鼓励政企单位使用国产安全浏览器

在安全浏览器领域，中国企业具有一定的先发优势。如360公司在2018年提出了企业安全浏览器的概念，并最早完成了规模化商业产品落地。该安全浏览器支持Windows全系列、MacOS全系列、信创平台全系列的操作系统。在信创平台的应用级产品层面，360企业安全浏览器与中国100多家应用厂商的产品实现了全面兼容。此外，中国企业具有的先发优势还表现在：

1）积极跟进了与浏览器相关的国际标准编制工作。2012年，以360为代表的中国安全公司加入万维网联盟（W3C）中最重要的超文本标记语言（HTML）工作组，与W3C共同研究和制定HTML5等新互联网标准；随后，加入全球CA/B根证书信任联盟。

2）发起了安全浏览器根证书计划。早在2018年，360公司就正式启动了公开密钥加密算法RSA（由发明者Rivest、Shmir和Adleman姓氏首字母缩写而来）根证书计划，与其他国家操作系统中的根证书库认证体系脱离，构建了自有的根证书审查机制，目前已完成全球100%权威CA机构的入根工作。在2020年360公司又启动了国密根证书计划。目前该计划已获得数十家中国CA机构的入根工作。这一举措是具有前瞻性的，这是因为在发生极端冲突时，一旦其他国家CA机构吊销用户网站证书，用户还可以利用360安全浏览器内嵌的安全可信根证书计划，立即重新建立网站访问信任，防止被“卡脖子”。

3）在技术上具有一定的创新性。和国际安全企业浏览器厂商相比，360安全浏览器具备大量的内置安全功能，包括数据丢失预防（DLP）功能、远程浏览器隔离（RBI）功能、安全访问控制功能、文件加密功能以及细化的认证和授权控制。该浏览器可面向Windows、Mac、信创等多个平台，提供统一的跨平台集约化管理方案，内置兼容性检测和修复工具，扩展应用商店、数据开放接口，提供安全方案咨询及定制化开发服务。

我们建议有关部门创造有利条件，发挥中国浏览器厂商已经取得的上述优势，从战略上重视并帮助安全浏览器厂商扩大生存空间，在数字经济、数字政府、数字城市等重要项目建设中，明确要求采用企业安全浏览器并限期全员部署，以保护中国数字工作空间入口。

3.2 发挥新型举国体制优势，打造自主战略级安全浏览器

浏览器是数字空间入口。一旦“断供”事件发生，中国数字空间的门户将敞开，因此我们建议应尽快制定中国企业安全浏览器的B计划（在积极跟踪Chromium浏览器开源内核的基础上，防止在未来极端情况下所面临的“卡脖子”风险），发挥新型举国体制优势，支持以科技领军企业为龙头，推动政府、市场与社会有机结合，集中各方力量进行攻关突破，打破技术垄断，从根本上解决中国各类数字应用的入口安全问题。

中国安全浏览器要获得长远发展一定离不开安全社区的建设。谷歌在开源社区方面的成功经验很值得中国借鉴：不论是实力强大的Chromium开源社区，还是开源供应链社区，均展现出娴熟利用社区力量推动技术和产业创新的卓越实践能力。未来，创新一定源于群体的力量，也一定驱动于不断提升用户体验的使命感。所以，培育安全浏览器社区文化，鼓励开发者创新，在创新中再回报开发者，才能获得真正的技术竞争优势。

3.3 加强安全浏览器人才培训，鼓励开展浏览器安全基础技术研究

目前，中国的安全浏览器是基于谷歌Chromium内核来开发的。Chrome浏览器拥有约2 300万行代码，因此构建企业浏览器是一件相当复杂的工作，需要大量安全专业人员投入和协同攻关。比如，微软Edge团队目前拥有1 000多名开发者，谷歌Chrome浏览器拥有一个2 000多人的开发团队。据粗略估算，中国从事浏览器开发工程师的数量不会超过500人，而具有浏览器内核开发能力的人才更少。实际上，目前中国安全浏览器开发方面的技术水平仅仅能跟上Chromium开源代码更新的速度。安全浏览器开发人才资源的严重不足将极大制约中国在该领域的创新和发展。因此，我们建议国家应加快制定针对安全浏览器的人才培养计划，并从科研项目、应用示范、

力量整合等方面加强浏览器安全基础技术研究，尽快实现中国在浏览器安全基础技术领域的突破。

参考文献

[1] CISA. Be cyber smart: get your “Shields Up” simple steps for safety online [EB/OL]. (2022-02-14) [2022-11-20]. https://www. cisa. gov/sites/default/files/publications/CISA_fact_sheet_4_things_Cyber_English_508.pdf

[2] Statcounter. Browser market share worldwide [EB/OL]. [2022-11-20]. https://gs.statcounter.com/browser-market-share

[3] MITRE corporation. CVE details [EB/OL]. [2022-06-06] [2022-11-20]. https://www.cvedetails.com/top-50-products.php

[4] Forrester. State of enterprise IoT security in north America: unmanaged and unsecured [EB/OL]. [2022-11-20]. https://info.armis.com/rs/645-PDC-047/images/State-Of-Enterprise-IoT-Security-Unmanaged-And-Unsecured.pdf

[5] Team8. Talon cyber security raises $26 million to develop next-generation cyber security for a distributed workforce [EB/OL]. [2022-11-20]. https://team8. vc/press-release/talon-cyber-security-raises-26-million-to-develop-next-generation-cyber-% E2%80%8B% E2%80%8Bsecurity-for-a-distributed-workforce/

[6] Wikipedia. Chromium (web_browser) [EB/OL]. [2022-11-20]. https://en.wikipedia.org/wiki/Chromium_(web_browser)

[7] Microsoft. Microsoft edge and bing maps [EB/OL]. [2022-11-20]. https://blogs. bing. com/search-quality-insights/may-2022/Turing-Image-Super-Resolution?s=09

[8] Microsoft. How can SmartScreen help protect me in Microsoft Edge [EB/OL]. [2022-11-20]. https://support. microsoft. com/en-us/microsoft-edge/how-can-smartscreen-help-protect-me-in-microsoft-edge-1c9a874a-6826-be5e-45b1-67fa445a74c8

[9] Microsoft. Chromium [EB/OL]. [2022-11-20]. https://microsoft. fandom. com/wiki/Chromium#Contributors

作 者 简 介

魏小强，360集团天枢智库研究员、国际云安全联盟（CSA）大中华区多云工作组组长、以色列Trusteer亚太区总经理、IBM大中华区高级安全专家、加拿大Entrust亚太区技术总监；拥有20年产品开发、运营管理、投融资、创业等经验；在边缘计算、零信任、多云安全、SASE、XDR、行为意识安全等领域拥有软著、专利、编著等20余个，发表论文多篇。

张义荣，360集团天枢智库负责人、高级工程师，中国网络空间安全协会个人信息保护专家组、网络安全产业统计调研专家组专家；具有16年以上行业经验，主要从事网络安全总体规划、体系设计、技术跟踪和产业研究等工作；完成国家自然科学基金、部委预先研究及重点工程建设等项目40余项；获部委级科技进步奖一等奖1项、二等奖4项、三等奖2项；发表学术论文30余篇。

黄亚洲，360数字安全集团浏览器业务线负责人；拥有17年产品开发和团队管理经验，擅长团队管理、战略规划、产品定义、市场布局等，开辟中国企业级浏览器品类赛道。