# Vulnerability chain assessment for multiple vulnerabilities

Deqiang Qiu[1, a], Sujuan Qin[2, b]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China;

[2] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China.

[a] aihaideqiu@sina.com, [b] 306118510 @qq.com

**Keywords:** CVSS, Vulnerability chain, Attack path.

**Abstract.** The dangers of a single vulnerability can be assessed by the CVSS, but in some cases, comprehensive harm of several vulnerabilities is 1 + 1> 2. So evaluating multiple vulnerabilities that are not just many single vulnerability assessments, but also integrated many complex situations. This paper studies the vulnerability chain score, an assessment of the attack path and do penetration testing laboratories to prove the validity of the assessment.

## 1. Introduction

Vulnerability is a key factor affecting network security, network vulnerability exists in all aspects of design implementation and operational management of the network. Completely eliminating all vulnerability is unrealistic and impossible. Practice shows that, although individual vulnerabilities affect a small number of isolated, but there are often links between vulnerabilities, If this link is a hacker exploit successfully and organized through a network, it may bring great harm to the network, which not only increases the concealment, but also increase the probability of a successful attack. But, Network vulnerabilities can analyze and measure the impact of network to identify high-risk vulnerabilities, and identify the association between vulnerability, thereby reducing the risk of vulnerability to attack by hackers use to reduce harm to the network. Network attack graph analysis of association between the vulnerability of the vulnerability assessment is significant, the exact correlation calculations will directly affect the outcome of the vulnerability assessment[1]

## 2. Chaining vulnerability

It's clear that Common Vulnerability Scoring System(CVSS) should always be scoped to individual vulnerabilities. But at the same time, vulnerabilities do not always exist (or get exploited) in isolation. Therefore, we hope to provide guidance on how to provide (and explicitly specify) CVSS scores for multiple related vulnerabilities. That is to say, when one or more vulnerabilities make conditions or resources available to an attacker that are required in order to exploit follow-on vulnerabilities that are also present, then it makes sense to derive a score for that chain of vulnerabilities.In some cases, chains will expose a series of low-impact vulnerabilities that result in a final, higher impact. In others, chains will describe how rollbacks, downgrades, or regressions in software can be exploited to reintroduce prior vulnerabilities from earlier, more vulnerable versions to newer software. In all cases, CVSS will require that each vulnerability be given its own, independent score. Then, the chain of vulnerabilities can be described and given a combined score for the chain itself. Chains might be described specifically (such as one CVE chained with one or more other CVEs) or generically (such as one or more vulnerability classes or CWEs being chained in order to exploit a specific CVE). But in the end, we believe that we could add value through CVSS to common scenarios without sacrificing the integrity of a scoring system that specifically addresses distinct vulnerabilities independent of each other.

In addition, the analyst may include other types of related vulnerabilities that could be chained with the vulnerabilities being scored. Specifically, the analyst may list generic types (or classes) of related vulnerabilities that are often chained together, or provide further descriptions of required preconditions that must exist. For example, one might describe how certain kinds of SQL Injection vulnerabilities are precursors to a cross-site scripting (XSS) attack, or how a particular kind of buffer overflow would grant local privileges. Listing the generic types or classes of vulnerabilities provides the minimum information necessary to warn other users, without potentially informing attackers about new exploit opportunities. Vulnerability A is: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H, and as can be seen from the vector, requires a local, low-privileged user in order to exploit. Whereas Vulnerability B is, AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L which provides an unprivileged, remote attacker the ability to execute code on a system with Low impacts if a local user interacts to complete the attack. Therefore, given both A & B, Chain C could be described as the chain of B -> A: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H which combines the Exploitability of B, the scope is unchanged in both cases, and the Impact of A, because if one can exploit B and gain the code execution as a local user from it, then one has satisfied the prerequisite to subsequently launch A causing an impact from vulnerability A.

## 3. Literature References

We experimentally analyzed how the chain vulnerability analysis.

In this paper, experimental network environment is similar to the literature [4] experimental network environment, shown in Figure 1.There are three hosts on the internal network, there is a firewall between the internal network and the external network. An attacker attempted invasion of the internal network.

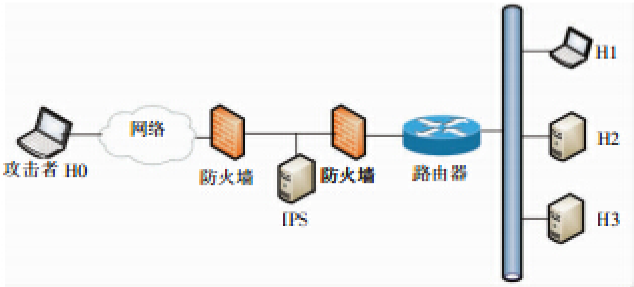

Fig. 1 Expermental network environment.

Experimental conditions known vulnerability shown in Table 1. Specific information for each ID as shown in Table 2.:

Table 1. Experimental network vulnerabilities cases

| PC | Services | Vulnerability ID |
|---|---|---|
| H1 | Workstation | A |
| H2 | Web Services（IIS 5.0）FTP Services | B、D、E |
| H3 | Oracle Services | C、F |

Table 2. Corresponding vulnerability information

| NO. | CVE ID | Description | Network | CVSS |
|---|---|---|---|---|
| **A** | CVE-2008-0076 | IEHTML rendering remote code execution vulnerability | Network | 9.3 |
| **B、E** | CVE-2006-0026 | IIS ASP Remote Buffer Overflow Vulnerability | Network | 6.5 |
| **D** | CVE-2008-0604 | Xlight FTP server LDAP authentication feature Access restriction bypass vulnerability | Network | 6.8 |
| **C、F** | CVE-2004-0385 | Oracle 9iAS / 10g Application Server Web Remote Heap Buffer Overflow Vulnerability | Network | 10 |

Use of CVE, we can get Corresponding CVSS vector:

C, F: AV: N /, AC: L /, PR: L /, UI: N /, C: H, / I: H, / A: H RC: Confirmed Technical details: Known

Intrusion detection capabilities: Unknown Date: 2004-04-09 time of approximately 4100 days ago

A: AV: N /, AC: H, / PR: N /, UI: R /, C: H, / I: H, / A: H RC: Confirmed Technical details: Known

Intrusion detection capabilities: Unknown Date: 2008-02-12 time of approximately 2700 days ago

B, E: AV: N, / AC: L, / PR: N /, UI: R, / C: L, / I: L, / A: L RC: confirmed technical details: has been disclosed

Intrusion detection ability: None Date: 2006-07-11 time is 3300 days ago

D: AV: N, / AC: L, / PR: N, / UI: R, / C: L, / I: L, / A: L RC: confirmed technical details: Unknown

Intrusion detection ability: None Date: 2008-02-06 time is 2700 days ago

Use Attack-path generate algorithm in Ref. [1], we can generate attack graph:

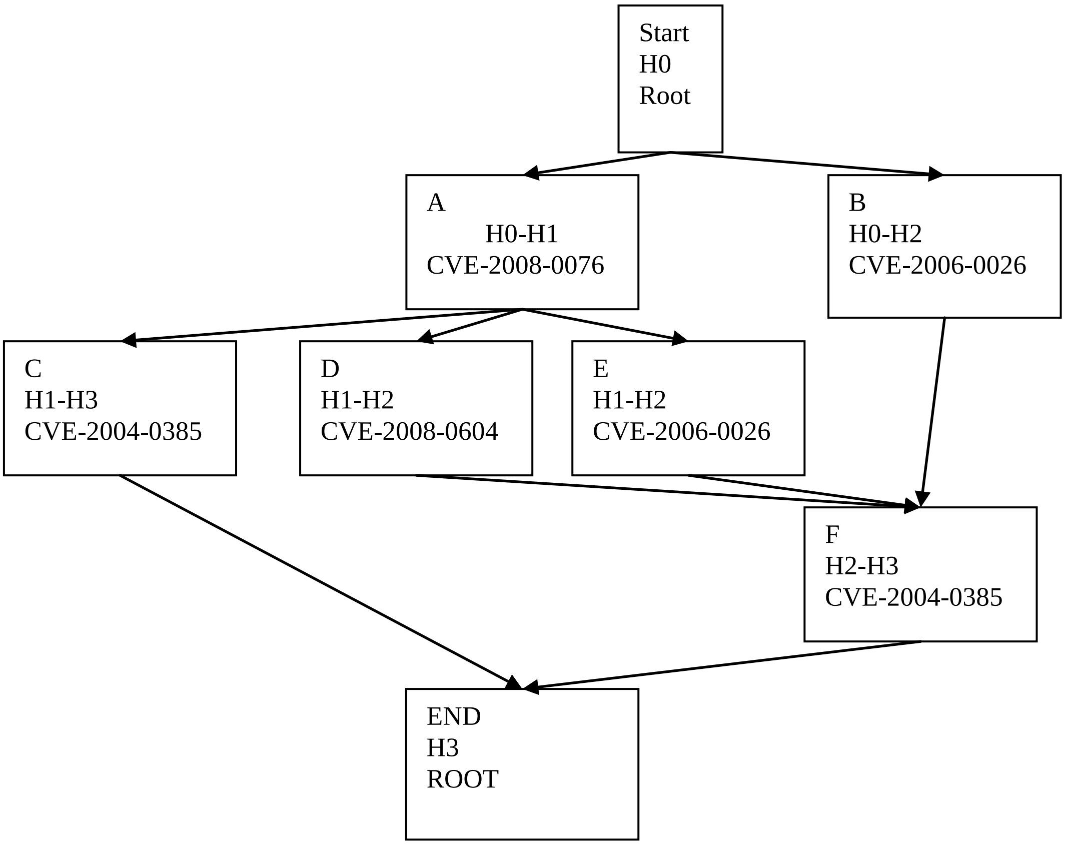

Fig.2 Attack Path

Then,Each node attack graph of the performance of the state where the attacker, the first column indicates the status of attackers taking advantage of loopholes in the process of the second column represents the attacker attacks the target host, the third column indicates the vulnerability is being used, or permission has been obtained.

According to the path attack graph displayed above, we can calculate the attack paths respectively.

Table 3. Vulnerability Chain Sorce

| Vulnerability Chain | Base source | Vector |
|---|---|---|
| **A->C** | 7.5 | AV:N/,AC:L,/PR:N/,UI:R/,C:H,/I:H,/A:H |
| **A->D->F** | 7.5 | AV:N/,AC:L,/PR:N/,UI:R/,C:H,/I:H,/A:H |
| **A->E->F** | 7.5 | AV:N/,AC:L,/PR:N/,UI:R/,C:H,/I:H,/A:H |
| **B->F** | 8.8 | AV:N/,AC:L/,PR:L/,UI:N/,C:L,/I:L,/A:L |

B:baseSorce=6.3,A:baseSource=9.3. So the best path to attack is B->F。

## 4. Summary

From the analysis of the actual situation of vulnerability, vulnerability A attack complexity is obviously higher than the vulnerability of B. A loophole is Internet Explorer 5.01, 6 SP1 and SP2, and Internet Explorer 7 parsing HTML with certain layout combinations in the way that there is a remote code execution vulnerability, an attacker by constructing a specially crafted Web page could exploit the vulnerability when a user view a Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. B is Microsoft IIS vulnerability in Microsoft Windows comes with a network information server, which includes HTTP services. Buffer overflow vulnerability exists on IIS implementation, a remote attacker could exploit this vulnerability to execute arbitrary commands on the server. A can use to get the current logged-on user privileges, but there is the difficulty of use of A, B albeit vulnerability to execute arbitrary commands. F vulnerability is a heap overflow issue exists

Oracle Web Cache all platforms, a remote attacker could exploit this vulnerability to authority service processes to execute arbitrary commands on the system. H2 B attack can exploit later, carefully constructed to submit data submitted 432 bytes long HTTP request method header request, can cause abnormal ntdll.RtlAllocateHeap error: to execute arbitrary commands on the system.

## ACKNOWLEDGMENT

This work is supported by NSFC (Grant Nos. 61300181, 61502044), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

## References

[1]. Xie Lixia, Jiang Dian Sheng, Zhang Li, etc. Assess Vulnerabilities Associated Method [J]. Journal of Computer Applications, 2012, 32(3):679-682. DOI:10.3724/SP.J.1087.2012.00679.

[2]. Zhang Feng Li, Feng Bo. Relevance vulnerability assessment method [J]. Journal of Computer Application Research,2014, 31(3). DOI:10.3969/j.issn.1001-3695.2014.03.042.

[3]. Gallon L, Bascou J J. Using CVSS in Attack Graphs.[C].2011 Sixth International Conference on Availability, Reliability and Security. IEEE Computer Society, 2011:59-66.

[4]. Zhang Xi, Huang Shuguang, etc. A vulnerability risk assessment approach based on attack graph [J]. Journal of Computer Application Research,2010, 27(1):278-280.

[5]. Liao Dan, Zhou Ming, Liu Dan, etc. An automatic optimization CVSSv2.0 assessment of the vulnerability index [J]. Computer Engineering and Applications, 2015, (2):103-107. DOI:10.3778/j.issn.1002-8331.1304-0133.